PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-254271
(43)Date of publication of application : 09.09.2004

(51)Int.Cl. H04L 9/08

(21)Application number : 2003-141286
(22)Date of filing : 20.05.2003

(71)Applicant : HITACHI LTD
(72)Inventor : MIZUTANI MIKA
KAMIMAKI HIDEKI
EBINA AKIHIRO

(30)Priority
Priority number : 2002375123 Priority date : 25.12.2002 Priority country : JP

(54) NETWORK INSTRUMENT, NETWORK SYSTEM, AND GROUP MANAGEMENT METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To realize secure communication between instruments belonging to a group which is constituted of instruments accepted by users.
SOLUTION: In a group management processing part 302, an encryption key used for cryptocommunication in a group is formed and stored in an own storage part and a storage medium together with information required for cryptocommunication. By using the storage medium, information required to perform cryptocommunication with oneself is transmitted to the other instrument which already belongs to the group. When leaving the group, information for performing cryptocommunication which the user himself owns is deleted, own leaving is informed to the other instruments, and information about the instrument to be leaving in the instruments which received notification is asked to be deleted. From instruments in the group, instruments selected by users are made a subgroup. An encryption key used for cryptocommunication in the subgroup is formed. Information required for cryptocommunication and subgroup information are transmitted to instruments belonging to the other subgroup by cryptocommunication using the encryption key of the group.

LEGAL STATUS

[Date of request for examination] 26.09.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1]

It is the network device which communicates with other network devices connected through the network,

The group management tool which manages as a group said network device of each other which can be attested,

A cryptocommunication means to perform cryptocommunication with a common encryption key between said network devices which carry out group affiliation,

A storage means to store cryptocommunication information required in order to perform the network device and cryptocommunication containing identification information including the host name and the address of a network device which belong to the information and said group of said encryption key which belong to said group,

It has an acquisition means to acquire information from the exterior,

Said group management tool,

If said cryptocommunication information is acquired in said acquisition means in the condition that said cryptocommunication information is not stored in said storage means, while storing the cryptocommunication information concerned in said storage means, own identification information is transmitted to the network device which belongs to said group through said cryptocommunication means,

said cryptocommunication means -- minding -- from other network devices -- being concerned -- others -- the network device which will be characterized by adding the identification information concerned to said cryptocommunication information memorized for said storage means if the identification information of a network device is acquired.

[Claim 2]

It is a network device according to claim 1,

Said group management tool is ,

If the directions which secede from a group in said acquisition means are received, while notifying balking of an own network device to all the network devices that belong to said group memorized by said storage means through said cryptocommunication means, said cryptocommunication information is deleted from said storage means,

said cryptocommunication means -- minding -- from other network devices -- being concerned -- others -- from said cryptocommunication information which will have been memorized for said storage means if the notice from which a network device secedes is received -- being concerned -- others -- the identification information of a network device is deleted

The network device characterized by things.

[Claim 3]

It is a network device given in either of claims 1 or 2,

Said acquisition means is the interface of a storage,

Said group management tool is ,

The network device characterized by copying the cryptocommunication information stored in said storage means to said storage when the storage with which said cryptocommunication information was stored is inserted in said acquisition means in the condition that said cryptocommunication information is stored in said storage means.

[Claim 4]

It is a network device given in either of claims 1, 2, or 3,

A non-cryptocommunication means to perform non-cryptocommunication,

It has further an access-control means to control access to the service which said network device offers,

Said access-control means is a network device characterized by permitting said access when it is a thing to the port where said access was beforehand defined when there was access from other network devices through said non-cryptocommunication means.

[Claim 5]

In the network system equipped with the network which connects two or more network device and said two or more network devices,

Said two or more network devices are network devices according to claim 1 to 4.

The network system characterized by things.
[Claim 6]
They are other devices connected through the network, and the group management method which manages the group who performs mutually cryptocommunication which can be attested,
The group generation step which holds the identification information which generates the encryption key used for said cryptocommunication in one device connected to said network, and includes the host name and the address of an encryption key and a self-device concerned as cryptocommunication information,
The 1st group participating step which notifies the information which shows own identification information and participation to the complete aircraft machine with which said identification information is stored in said cryptocommunication information in the device which acquired said cryptocommunication information by said cryptocommunication, and adds and holds own identification information to the cryptocommunication information concerned,
The 2nd group participating step which adds the identification information concerned to said cryptocommunication information which self holds in the device which received the information which shows the identification information concerned and said participation,
The 1st group balking step which deletes said cryptocommunication information which notifies the information which shows balking to the complete aircraft machine with which said identification information is stored in said cryptocommunication information except self in the device which received the directions which secede from said group, and own identification information by said cryptocommunication, and self holds,
The group management method characterized by having the 2nd group balking step which deletes the identification information which received the notice from said cryptocommunication information which self holds in the device which received the notice of the balking concerned.
[Claim 7]
Computer,
A group generation means to hold the identification information which generates the encryption key used for cryptocommunication and includes the host name and the address of the encryption key concerned and self as cryptocommunication information,
The 1st group participating means which notifies the information which shows own identification information and participation to the complete aircraft machine with which said identification information is stored in said cryptocommunication information when said cryptocommunication information is acquired by said cryptocommunication, and adds and holds the identification information of said self to said cryptocommunication information,
The 2nd group participating means which will add the identification information

concerned to said cryptocommunication information which self holds if the information which shows the identification information of other devices to the device concerned and participation is received,
The 1st group balking means which deletes said cryptocommunication information which notifies the information which shows balking to the complete aircraft machine with which said identification information is stored in said cryptocommunication information except self when the directions which delete said cryptocommunication information are received, and the identification information of said self by said cryptocommunication, and self holds,
The 2nd group balking means which deletes the identification information which received from said cryptocommunication information which self holds when the information which shows the identification information of other devices and said balking was received,
The program for making it function by carrying out.
[Claim 8]
It is a network device according to claim 1 or 2,
The network device contained in the 1st group connected to said network is displayed, and it has a selectable interface means,
Said group management tool manages said selected network device as the 2nd group,
Said storage means stores the cryptocommunication information containing identification information including the host name and the address of the network device which belongs to said the 2nd encryption key and said 2nd group,
Said cryptocommunication means is a network device characterized by performing cryptocommunication with the 2nd common encryption key into said 2nd group.
[Claim 9]
It is a network device according to claim 8,
The network device characterized by having a means to transmit said cryptocommunication information enciphered using said 1st group's encryption key to the network device which belongs to said 2nd group.
[Claim 10]
It is a network device according to claim 8,
Said storage means is stored as said 2nd group's cryptocommunication information, when said cryptocommunication information enciphered with said 1st group's encryption key is acquired from other network devices,
The network device characterized by performing the 2nd group communication link by the cryptocommunication using said 2nd cryptographic key.
[Claim 11]
It is a network device according to claim 8,
Said interface means by which a user can set up the 2nd user-identification information and confidential information corresponding to a group,
Said storage means to store group information which consists of said user-

identification information, confidential information, said 2nd group's cryptocommunication information, and an authentication key generated in the 2nd corresponding group identification descriptor and the corresponding self-network device,
A means to store said 2nd group information in a storage,
Said 2nd group information is enciphered with said 1st group's encryption key, and it has a means to transmit to all the network devices belonging to the 2nd group.
Said storage means is a network device characterized by storing said group information decrypted using said 1st encryption key, when said 2nd enciphered group information is received.
[Claim 12]
It is a network device according to claim 11,
A means to check that it is the same as that of the value memorized by said storage in the user-identification information which the self-device has managed, and confidential information,
It has a means to search the 2nd cryptographic key which the device corresponding to the group identification information memorized by said storage manages,
The network device characterized by performing cryptocommunication among said 2nd group using said 2nd cryptographic key.
[Claim 13]
Claims 8 or 11 are the network devices of a publication either,
The network device which has said interface means is a network device characterized by decrypting using said 1st encryption key and storing said group information in said storage means when said 2nd enciphered group information is received.
[Claim 14]
Claims 8 or 11 are the network devices of a publication either,
A storage means to store the transmitting agency port number of said application when starting the application which needs the communication link with other network devices belonging to said 2nd group,
When a packet is transmitted from said application, it has a means by which said management port number remembered to be the transmitting agency port number of said packet checks coincidence,
The network device by which it is transmitting [said packet]-by the 2nd group communication link by cryptocommunication using said 2nd cryptographic key only in case of being in agreement characterized.
[Claim 15]
In the network device of any of claims 8 or 11, or a publication,
The network device characterized by having a storage means to add and store in a front storage the address of the network device which stores said group information in said storage.
[Claim 16]

In the network device of any of claims 8 or 11, or a publication,
While storing said group information in said storage,
The network device characterized by carrying out additional storing of the identifier and the address of all the network devices belonging to said 2nd group at said storage.
[Claim 17]
It is the network system characterized by said two or more network devices being one network devices of claim 8 to claims 16 in the network system equipped with the network which connects two or more network device and said two or more network connection devices.
[Claim 18]
In the network system to which the 1st network device which performs a group communication link, and the 2nd network device which does not perform a group communication link are connected,
Said 2nd network device,
The means which reads the user-identification child, the confidential information, the group identification descriptor, the authentication key, and the address on a storage through a storage according to claim 15,
An interface means by which a user inputs a user-identification child and confidential information,
A means to check that the value which inputted the user-identification child and confidential information on a storage is in agreement,
A means to encipher said user-identification child and confidential information with an authentication key, and to transmit said user-identification child who enciphered, and confidential information and a group identification descriptor to said addressing to the address,
It has a means to receive the 2nd common encryption key enciphered with said authentication key,
The network device characterized by performing cryptocommunication with said 2nd common encryption key when said user communicates.
[Claim 19]
In the 2nd network device according to claim 18,
A means to display the identifier and the address of a network device on a storage on a user through a storage according to claim 16,
A means to choose a network device to connect from the network device by which the user was displayed,
The network device characterized by having a means to transmit the user-identification child who enciphered with the authentication key on a storage to the address of the network device which the user chose, and confidential information and a group identification descriptor.
[Claim 20]
Claims 18 or 19 are the network devices of a publication either,

Said 1st network device,
A means to receive said user-identification child who enciphered, and confidential information and a group identification descriptor in said 2nd network device,
A means to search the authentication key which becomes the group identification descriptor managed by the device, and a pair from said group identification descriptor which received,
A means to decrypt confidential information with a user-identification child using said authentication key,
A means to check whether confidential information is in agreement with a group identification descriptor and the user-identification child who manages by the corresponding device,
The 2nd common encryption key managed by the device which becomes said group identification descriptor and pair is enciphered with said authentication key, and it has a means to transmit to the 2nd network device,
The network device characterized by performing an encryption communication link with the 2nd common encryption key to the communication link with the 2nd network device.
[Claim 21]
It is a network system,
The network device according to claim 20 which performs a group communication link, and claims 18 or 19 which do not perform a group communication link are the network system characterized by connecting the network device of a publication either.
[Claim 22]
It is a group management method according to claim 6,
The selection step as which the network device belonging to a group is chosen, other encryption keys each other used for the cryptocommunication which can be attested between said selected network devices -- generating -- being concerned -- others -- the host name of an encryption key and the network device belonging to said 2nd group, and the 2nd group coding information generation step which holds the cryptocommunication information containing identification information including the address,
The 2nd group coding information distribution step which notifies said cryptocommunication information to the network device which enciphers using said encryption key and belongs to said 2nd group,
The group participating step to which the device which received said 2nd cryptocommunication information holds the 2nd cryptocommunication information concerned,
The 2nd group information generation step which holds user-identification information, the confidential information which the user created, said 2nd group's cryptocommunication information, the 2nd corresponding group identification descriptor, and group information that consists of a generated authentication key, and

stores said information in a storage,
The 2nd group information distribution step notified to the network device which enciphers the 2nd group's group information and belongs to said 2nd group using said encryption key,
The group management method characterized by having the group access privilege setting step to which the device which received said 2nd group information holds said group information.
[Claim 23]
It is a group management method according to claim 22,
The user authentication step to which the user-identification information and confidential information which the device has managed check that it is the same as that of the value on said storage,
The group management method characterized by having the cryptocommunication preparation step which holds the port number of application.
[Claim 24]
In a program according to claim 7,
A selection means by which the network device belonging to a group is chosen,
The 2nd group coding information generation means which memorizes the cryptocommunication information containing identification information including the host name and the address of the network device which generates the encryption key each other used for the cryptocommunication which can be attested, and belongs to an encryption key and said 2nd group concerned between said selected network devices,
2nd group coding information distribution means to encipher the 2nd group's cryptocommunication information and to notify to the network device which belongs to said 2nd group using said encryption key,
A group participating means to hold cryptocommunication information in the device which received said 2nd cryptocommunication information,
User-identification information, the confidential information which the user created, said 2nd group's cryptocommunication information, and the 2nd corresponding group identification descriptor, And the 2nd group information generation means which memorizes group information which consists of a generated authentication key, and stores said information in a storage, 2nd group information distribution means to encipher the 2nd group's group information and to notify to the network device which belongs to said 2nd group using said encryption key,
A group access privilege setting means to memorize group information in the device which received said 2nd group information,
A user authentication means to check that it is the same as that of the value on said storage in the user-identification information and confidential information which the device has managed through said storage when a user uses a network device,
A cryptocommunication preparation means to hold the port number of the application

which a user uses,
A means to perform cryptocommunication with the 2nd group's encryption key when in agreement, if the port number of a transmitting packet holds when carrying out packet transmission to the device belonging to the 2nd group,
The program for making it function by carrying out.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
This invention relates to exclusive between the specific devices linked to a network, and the technique which communicates safely.
[0002]
[Description of the Prior Art]
Internet IP network which uses the communications protocol called Protocol (hereafter referred to as IP) establishes the status as a de facto standard of a computer network, and its spread in a general user is remarkable.
[0003]
In order to exchange data between devices through this IP network, it is required for each of that device to give an IP address uniquely. Although IPv4 (Internet Protocol version 4) which expresses an IP address with 32 bits is used in current, use of IP network takes for increasing and is posing the problem that lack of an IP address is big.
[0004]
Against the background of such a situation, an IP address is extended to 128 bits, IPv6 (Internet Protocol version 6) is adopted in IETF (Internet Engineering Task Force) as an IP network using the new IP address which added further the function which was not in old IP addresses, such as a security function, and the network service using it is being standardized as the next generation IP.
[0005]
Furthermore, the usable number of the addresses increases and the home network which consists of domestic devices called AV equipments, such as white home appliances, such as a refrigerator and a washing machine, or television, and video, attracts attention as a new application place of IPv6 in which the security function was substantial.
[0006]
It considers being able to consider now that each device is a server, and the

communication link between devices realizing new service, or realizing new service through the Internet, such as control of the device from an external terminal, and control of the device from a service center, by IP address quota ******, to each of these devices.

[0007]

By the way, in the communication link between specific devices like a domestic device, a system which eliminates the actuation from the device out of range which the user recognizes is required. For example, the selfish actuation by the device which the friend brought needs to be prevented.

[0008]

That is, a user determines the range which permits a mutual communication link, and a system by which grouping of those devices is carried out, and a communication link is made only between the devices by which grouping was carried out is required. And in order to realize such a communication link, the authentication function for attesting that it is the Shinsei device which belongs each other in a group between the devices in a group is required.

[0009]

As such an authentication function, what used the authentication server is realized in the conventional client and the system of a server mold. For example, in RADIUS (Remote Authentication Dial-In User Service) defined by RFC2865, it judges whether package management of the account (a user name, password) of the client which accesses a server is carried out by the authentication server called a RADIUS server, a server transmits the access request (a user name and a password are included) from a client to a RADIUS server, and the communication link with a client is performed in response to the decision result of access propriety.

[0010]

For example, as the cryptocommunication system and its correspondence procedure between the conventional specific devices by which grouping was carried out, there are some which are shown in the patent reference 1 or the patent reference 2, for example.

[0011]

[Patent reference 1] JP,2002-124941,A

[Patent reference 2] JP,5-347616,A

[0012]

[Problem(s) to be Solved by the Invention]

In order to perform a communication link predetermined only between the devices specified by a user in the device connected to the home network, the function which attests that it is the device by which the partner of each other was specified is considered to be the need.

[0013]

A client/server system is a premise and the conventional authentication function is

realized by having the authentication server which manages the access information of the client which accesses a server.

[0014]

On the other hand, the device which constitutes a home network is the ad hoc mold of communicating between required devices according to service suitably. For this reason, there is a problem that all devices can become a server and a client and a setup of access information becomes more complicated.

[0015]

In such a case, when it has an authentication server like before and is made to attest according to an individual for every session activation between devices, and every service initiation, there is also a problem that the overhead of authentication becomes large.

[0016]

For example, the technique indicated by the above-mentioned patent reference 1 is group communication system with an authentication function. This technique reaches with the group cryptographic key Management Department having the function to manage the terminal information which belongs in group communication system at the function and group who generate a group cryptographic key in addition to the device which constitutes a group, it is equipped with repeating installation, is constituted and is premised on large-scale network configuration.

[0017]

Moreover, the technique indicated by the above-mentioned patent reference 2 must possess the IC card first for every device which performs a group communication link. And two or more master keys and group key generators which were beforehand set up for every affiliation of a transceiver partner need to be recorded on the IC card.

[0018]

Thus, in the Prior art, the device which serves as an authentication server in addition to the device which actually communicates needed to be prepared, and only the number of the devices which constitute a group needed to prepare the record medium which makes the complicated information of the relation between a master key and each communications-partner point memorize beforehand.

[0019]

Since use of the device by the third person cannot be barred even if it constitutes the group of a device, it attests between the device and it realizes a safe communication link, selfish actuation which a user does not expect may be performed. That is, there is a problem that the access control of the user level using the user using a group and a device cannot be performed.

Moreover, there is a problem that the device which can be used by the user cannot be restricted, either.

In addition, it is applicable only to a communication link between the devices arranged at the local network to which the location was fixed called a domestic network. Since

this uses IPsec, in order to judge whether it is the device which constitutes a group, in addition to a share key, it is based on that the pair of a transmission place IP address and a receiving agency IP address needs to be immobilization. When the device which constituted the group moves from a local network, the technical problem that the access control by group communication link is inapplicable occurs.

[0020]

This invention was made in view of such a situation, and the purpose of this invention constitutes the group who can attest each other mutually easily between the devices which the user accepted, and is to realize the safe communication link between the devices belonging to the group.

[0021]

Furthermore, other purposes of this invention are to realize the access control of permitting access only to the application, from the device besides a group, when some which also permit access to the device besides a group are in the application which the device in a group offers.

[0022]

Other purposes of this invention are realizing the access control of the user using a subgroup while constituting the subgroup which limits a user in the group who constituted between the devices which the user accepted.

[0023]

Other purposes of this invention are to realize safe access/control to the device which constitutes a subgroup from the place which the distance with a physical user left.

[0024]

In addition, this application solves at least one of the above-mentioned purposes.

[0025]

[Means for Solving the Problem]

This invention attests each other by performing cryptocommunication using a shared key, considers that the assembly of a device which performs the communication link from which security was secured is a group, and has the means of group management of each [each device] and generating a group, and participating and seceding from the group which can serve as a device which constitutes the group.

[0026]

Moreover, even if the device belongs to one of groups, the possibility of the communication link with the device besides a group is also held.

[0027]

The group management tool which is the network device which specifically communicates with other network devices connected through the network, and manages as a group said network device of each other which can be attested, A cryptocommunication means to perform cryptocommunication with a common encryption key between said network devices which carry out group affiliation, A

storage means to store cryptocommunication information required in order to perform the network device and cryptocommunication which belong to said group including identification information including the host name and the address of the network device which belongs to said group, and the information on said encryption key, and an acquisition means to acquire information from the exterior, A preparation and said group management tool are in the condition that said cryptocommunication information is not stored in said storage means. If said cryptocommunication information is acquired in said acquisition means, while storing the cryptocommunication information concerned in said storage means the network device which belongs own identification information to said group through said cryptocommunication means -- transmitting -- said cryptocommunication means -- minding -- from other network devices -- being concerned -- others, if the identification information of a network device is acquired The network device characterized by adding the identification information concerned to said cryptocommunication information memorized for said storage means is offered.
[0028]
Moreover, if the directions which secede from a group in said acquisition means are received further, said group management tool While notifying balking of an own network device to all the network devices that belong to said group memorized by said storage means through said cryptocommunication means said storage means to said cryptocommunication information -- deleting -- said cryptocommunication means -- minding -- from other network devices -- being concerned -- others, if the notice from which a network device secedes is received from said cryptocommunication information memorized for said storage means -- being concerned -- others -- the network device characterized by what the identification information of a network device is deleted for is offered.
In the network device which constitutes said first group, choose the network device which a user can use, and said cryptocommunication means is minded to these devices. By distributing the second cryptographic key used by the selected network device, the second group is constituted in the first group, by performing cryptocommunication using the second common cryptographic key, each other is attested and the communication link from which security was secured is performed. Moreover, while managing the second cryptographic key, the corresponding user's identifier, and the information on a password with a network device and a storage By distributing to the network device which enciphers said information by the first cryptographic key, and performs other second group communication link In case a user uses a network device, in every network device, the access control of the use propriety of a group communication link is offered by checking that the information on a storage and the information on a network device are in agreement.
By requesting management to the network device which manages the address and the authentication key of a network device with a storage, manages an authentication key

in a network device, enciphers by the first cryptographic key, and performs other second group communication link In case a user starts the network device second for a group communication link, and a communication link from the network device which is not a candidate for a group communication link, with the authentication key of a storage Encipher the password and user ID of a storage and the encryption information is transmitted to addressing to the address of a storage. After decrypting user ID and a password with the authentication key by the network device second for a group communication link and checking user ID and a password The cryptocommunication in the second cryptographic key is offered by enciphering and returning the second common cryptographic key with an authentication key between the network devices which are not the candidates for a group communication link.
[0029]
[Embodiment of the Invention]
Hereafter, the gestalt of operation of this invention is explained using drawing.
[0030]
The case where this invention is applied to the network constituted by household electric appliances etc. in ** is mentioned as an example, and this operation gestalt explains it.
[0031]
The network in ** of this operation gestalt is constituted by IPv6, the IP address was given to each, for example, AV equipments, such as household-electric-appliances devices, such as a microwave oven and an air-conditioner, television, and video, a sensor, etc. are connected to it. Hereafter, it connects with a network and suppose that each device to which the IP address by IPv6 is given is called a node.
[0032]
With this operation gestalt, what permitted that a user communicated mutually among these nodes is made into a group, and cryptocommunication with an encryption key common for authentication between the nodes belonging to a group is performed. While the structure of the code and authentication called IPsec is equipped as standard and the securable number of IP addresses not only becomes immense [IPv6 adopted in this network] as mentioned above, but it maintains advanced safety here, it has the description of being user-friendly. In this operation gestalt, the safe communication link only between the devices which constitute a group is realized using IPsec of IPv6.
Before detailed explanation of this operation gestalt, the outline of IPsec is explained first.
IPsec is the technique of offering the security of the encryption base it being able to interconnect and quality in IP layer. This security is realized by two traffic security protocols, the authentication header AH (Authentication Header) and IP encryption payload ESP (Encapsulation Security Payload), etc.
[0033]

It is AH's offering the function which prevents the alteration of an IP packet, and ESP's enciphering an IP packet, and storing the authentication data, and the confidentiality and integrity of an IP packet are guaranteed.

[0034]

The device of a communications partner is attested by whether the key which can decode the enciphered data with which AH and ESP created and sent authentication information and code data using the authentication key and the cryptographic key, respectively is held.

[0035]

The configuration of the IP packet at the time of using AH protocol and an ESP protocol for drawing 4 and drawing 5 , respectively is shown. In addition, these packet configurations are specified to RFC 2401-2403 as an IPsec packet.

[0036]

Drawing 4 shows the configuration of the IP packet at the time of using AH protocol. The IP packet in this case is equipped with the IP header 400, the TCP/UDP header 402, and the AH header 401 that stores the hash value to data 403.

[0037]

The hash value stored in the AH header 401 is for proving that the packet is not altered, and the value calculated using the authentication key mutually held between communications partners is stored. As compared with the hash value of the data to which the receiving side calculated the hash value of the data which calculated this with the authentication key which self holds by the transmitting side by it being the requisite to hold the authentication key same what are attested, and were stored with the authentication key which self holds, when both agree, a partner can check that it is what holds the same authentication key. That is, it is proved that it is a device in the group in whom the transmitting partner of a packet holds the same encryption key.

[0038]

Drawing 5 shows the configuration of the IP packet at the time of using an ESP protocol. It is a header configuration at the time of enciphering data as a TCP/UDP header.

[0039]

The IP packet in this case is equipped with the ESP trailer 504 and the authentication data 505 for arranging the break of encryption with the ESP header 501 which shows that it is the enciphered packet. The authentication data 505 are an option and store the hash value of the ESP header 505, the enciphered TCP/UDP header 502, data 503, and the ESP trailer 504.

[0040]

The hash value stored in the authentication data 505 secures the confidentiality of the TCP/UDP header 502 which secures the integrity of IP payload, enciphers and is transmitted, and data 503. In case it enciphers, the cryptographic key which a transmitting side holds is used. It decodes by the cryptographic key in which, as for a

receiving side, self holds the data which the transmitting side enciphered using the cryptographic key which self holds. In a receiving side, if decode is possible, it can check that a partner holds the same cryptographic key. That is, a packet transmitting partner becomes the certification of being the device in a group which holds the same cryptographic key.

[0041]

Moreover, the information which should be shared in order to communicate according to the specification of IPsec among each devices, such as a code / authentication algorithm, a key, etc. which are used by IPsec, (the thing of the communication link performed according to the specification of IPsec is henceforth called an IPsec communication link) is managed as a security association (SA).

[0042]

SA is a "connection" of an one way who offers security service to the traffic carried by it. For this reason, in performing an IPsec communication link, it is necessary to set up beforehand for every communication link of an one direction between the devices which communicate. That is, in order to communicate both directions, it is necessary to set up each SA of a transmit direction and a receive direction.

[0043]

In addition, the detail of IPsec is specified to RFC2401"Security Architecture for the Internet Protocol."

[0044]

Drawing 1 is drawing showing the configuration of the group communication system concerning 1 operation gestalt which applied this invention.

[0045]

As shown in this Fig., in this operation gestalt, four nodes 100 (100A, 100B, 100C, 100D) are connected to the network 110 by IPv6. Of course, the number of configuration nodes is not restricted to this.

[0046]

Actuation from other nodes 100 to the service function peculiar to a device with which node 100 each is equipped, and service provision to other nodes 100 are realized by transmitting and receiving the command of an IP packet format through a network 110 among these nodes 100.

[0047]

The image which carries out temperature control of an air-conditioner from television, or is photoed with the video camera by actuation from television through a network is specifically transmitted to video, and making the image photoed with the video camera record on videotape by video is realized.

[0048]

For example, node 100A – node 100C It is a node belonging to the group who has permitted that a user uses service mutually. Node 100D If it is a node besides the group, between the nodes 100A and 100B which constitute a group, and 100C In case

the use demand of a service function is transmitted, the requiring agency node stored the hash value calculated with the key (it is henceforth called a group key) shared between a group, or sends the enciphered IP packet (101 directions). a requiring agency node is a group configuration node by the group key with which self holds the demand place node which received the use demand -- checking -- a service function -- a requiring agency node -- providing (102 directions) -- the said IPsec communication link is performed.

[0049]

On the other hand, when the use demand of a service function transmits the usual IP packet to node 100C in order to transmit by the usual IP packet (104 directions), it will be judged to be a node outside a group in node 100C, and will receive answerback of the packet of service provision refusal from node 100D (103 directions).

[0050]

Here, if in the case of the node which has the service in which node 100B permits offer to the node 100 besides a group offer of the service is specified from node 100D and the usual IP packet is transmitted (the direction of 104b), the service will be offered from node 100B (the direction of 103b).

[0051]

The network in which the communication link by the protocol using IPv6 which mounts the structure of IPsec as standard as mentioned above is possible is mentioned as an example, and this operation gestalt explains it. However, an encryption key common between the nodes 100 which constitute a group is given, and if the environment which can communicate between groups involved by making the key into an authentication key or a cryptographic key can be built, a communications protocol will not be restricted to this.

[0052]

A group is generated, other nodes 100 participate and how to secede from the generated group is explained to the generated group in the management method 100 of the group who realizes safe use of predetermined service between the nodes 100 hereafter connected to such a network, i.e., one node.

[0053]

With this operation gestalt, two of the empty memory cards A and B are prepared, information required in order to perform an IPsec communication link within a group is generated in the node 100 which participates in a group first, and it registers with one of the memory cards [them] A. The node 100 which participates after that is acquiring required information from a memory card A, and participates in a group. Moreover, in case it secedes from a group, the empty memory card B is used.

[0054]

The hardware configuration of a node 100 is shown in drawing 2 , and the functional configuration is shown in drawing 3 .

[0055]

A node 100 is equipped with the system bus 203 which connects these with the processor 200 which controls one or more proper function parts 202 with which a node 100 is equipped, network card 205, and the proper function part 202 and a network card 205, the memory 201 which memorizes the program performed by the processor 200, the external storage 204, such as a hard disk which memorizes a program and setting information, and the storage interface 206 which offers interfaces, such as a memory card for delivering group information.

[0056]

In addition, if the proper function which the proper function part 202 realizes is an air-conditioner, they are things, such as the processing section which manages an air conditioning function, a temperature function manager, timer ability, etc., for example.

[0057]

Moreover, the storage interface 206 possesses LED (light emitting diode) Wright who writes in the storage to insert and notifies a user of it being inside.

[0058]

Next, the function with which each node 100 is equipped is explained according to drawing 3 . By these functions, a node 100 realizes offer of service through a network between the nodes 100 which constitute the group whom the user permitted mutual use of service.

[0059]

Each node 100 is equipped with application 301, the group management processing section 302, the TCP/UDP transmitting processing section 303, the IP transmitting section 304, the access polish database 308, the SA database 309, the network interface reception section 310, the IP receive section 314, the TCP/UDP reception section 315, the network interface transmitting processing section 317, and the storage interface processing section 318.

[0060]

Application 301 offers service peculiar to each node.

[0061]

As for the group management processing section 302, a group's generation mentioned later, balking, updating, etc. perform management about a group.

[0062]

The network interface reception section 310 and the network interface transmitting processing section 317 control a network card.

[0063]

The storage interface processing section 318 controls the storage interface 206. When it detects that record media, such as a memory card, were inserted in the record-medium interface 206, the storage interface 318 turns on LED Wright with whom the storage interface 206 is equipped, and shows to a user that a memory card is under use. Moreover, if the notice of processing termination is received from the group management processing section 302, LED Wright with whom the storage

interface 206 is equipped will be switched off, and it will notify that the writing to storages, such as a memory card, was completed, and that the processing in the group management processing section 302 was completed to a user.
[0064]
In addition, the user who received the notice can take out a memory card from the storage interface 206 concerned.
[0065]
To the IP packet sent and received, the TCP/UDP transmitting processing section 303, the IP transmitting section 304, the IP receive section 314, and the TCP/UDP reception section 315 process each class, and realize a communication link.
[0066]
The IP transmitting section 304 is equipped with the IPv6 transmitting pretreatment section 305, the IPsec transmitting processing section 306, and the IPv6 after-treatment section 307, and the IP receive section 314 has the IPv6 reception pretreatment section 311, the IPsec reception section 312, and the IPv6 receiving after-treatment section 313. The communication link by IPv6 is realized in the IP transmitting section 304 and the IP receive section 314.
[0067]
Here, the IPv6 reception pretreatment section 311 performs IPv6 reception pretreatment called the check of the set point and option header (except for AH and ESP) processing of the version which constitutes IP header, payload length, and a hop limit. The IPv6 reception pretreatment section 311 delivers the IP packet to the IPsec processing section 312, when either AH header or the ESP header is added to the received IP packet. When neither of the headers is added, it delivers to the receiving access-control section 316 which mentions the IP packet later.
[0068]
The IPsec processing section 312 judges whether it is what was transmitted from the node 100 to which the IP packet which performed processing of AH and ESP among the option headers of IP header, and received belongs to a group.
[0069]
The IPv6 receiving after-treatment section 313 is Pusedo including a transmitting agency IP address and a transmission place IP address, when an IP packet is received. Header is created, it replaces with IP header of the received IP packet, and IPv6 receiving after treatment of delivering to the TCP/UDP reception section 315 is performed. Moreover, the IP receive section 314 has the receiving access-control section 316 further.
[0070]
The receiving access-control section 316 controls reception and access to the application of the IP packet concerned for the IP packet which does not have AH header or the ESP header from the IPv6 reception pretreatment section 311.
[0071]

The security association (SA) which needs the SA database 309 at IPsec is stored.
[0072]
In order that the access polish database 308 may realize a communication link within a group, the information and group information about the access control to each node are stored.
[0073]
The access polish database 308 is equipped with the group managed table 600, the application managed table 700 for an access control, and the group member managed table 800.
[0074]
In addition, the group managed table 600 is held also on the memory card which is the storage connected to a node through the storage interface 206.
[0075]
Hereafter, the detail is explained about SA in each database of the group management processing section 302 and the access polish database 306, and the SA database 309.
[0076]
The functional block diagram of the group management processing section 302 is shown in drawing 6 .
[0077]
As shown in this Fig., the group management processing section 302 is equipped with a control section 3100, the group generation processing section 3200, the group participating processing section 3300, the group balking processing section 3400, the group information update process section 3500, and the group control IP packet reception section 3600.
[0078]
The group management processing section 302 starts processing with the directions from the storage interface processing section 318 which detected that the user inserted the memory card in the storage interface 206.
[0079]
A control section 3100 searches the access polish database 308 which receives the directions from the storage interface processing section 318, and self holds in the inserted memory card, and checks the existence of the group managed table 600.
[0080]
The group generation processing section 3200 performs group generation processing which newly generates a group, when the group itself does not exist. Group generation processing is performed when it is judged that a control section 3100 does not exist in a memory card, either, and the group managed table 600 does not exist in the access polish database 308, either.
[0081]
Information required in order to specifically perform other nodes and cryptocommunication belonging to a group, i.e., the item which should be registered

into the group managed table 600, is generated and chosen, the group managed table 600 is created, and it is registered into a memory card and the access polish database 308.

[0082]

The group participating processing section 3300 gives the existing group group participating processing in which self is made to participate as a new member. Group participating processing is performed when a control section 3100 judges that the group managed table 600 does not exist in the access polish database 308 although the group managed table 600 exists in a memory card.

[0083]

The group participating processing section 3300 transmits information required in order to acquire information required for the cryptocommunication stored in the inserted memory card and to perform an own node 100 and cryptocommunication to other nodes 100 which already belong to the group. The group managed table 600 to which the information on own was added to the group managed table 600 in a memory card, and the information on own was specifically added is registered into the access polish database 308.

[0084]

Moreover, the group member managed table 800 is generated by solving an IP address from the host name of the node 100 which was obtained from the group managed table 600 and which already belongs to the group.

[0085]

Furthermore, the group participating processing section 3300 sets up a security association, registers it into the SA database 309, and notifies that self was added to the node 100 of the existing member in a group by the IPsec communication link so that each node 100 in a group and an IPsec communication link may be attained.

[0086]

The group balking processing section 3400 performs group balking processing in which it secedes from a group.

[0087]

With this operation gestalt, when a user wants the predetermined node 100 to secede from a group, suppose that an empty memory card is inserted in the node 100 concerned. That is, it is carried out when group balking processing is judged that the group managed table 600 does not exist in the memory card in which the control section 3100 was inserted although the group managed table 600 existed in the own access polish database 308.

[0088]

It notifies that the own node 100 secedes from group balking processing to other nodes 100 belonging to a group, and the data concerning the communication link between the groups in the information 308 required in order to perform cryptocommunication within groups involved, i.e., an own access polish database, and

the SA database 309 are deleted.
[0089]
Here, in case the group participating processing section 3300 and the group balking processing section 3400 notify participation and balking to each node 100 belonging to a group, respectively, the IP packet which has the special data division called a group control IP packet is used.
[0090]
Here, the group control IP packet is explained. An example of the data division 1000 of a group control IP packet is shown in drawing 7 .
[0091]
As shown in this Fig., the data division 1000 of a group control IP packet are equipped with 16 bytes of IP address storing section 1002 which stores the command identifier storing section 1001 which stores a command identifier, and an IP address and a host name, respectively, and the host name storing section 1003.
[0092]
Here, in case new participation is notified, in the case of the group control IP packet transmitted to each node 100 belonging to a group, (00) hex which shows "subscription" is set as the command identifier storing section 1001 (this group control IP packet is henceforth called a subscription command). And the own address and an own host name are set to the IP address storing section 1002 and the host name storing section 1003, respectively.
[0093]
Moreover, in case it secedes from a group, in the case of the group control IP packet transmitted to each node 100 belonging to a group, (01) hex which shows "balking" is set as the command identifier storing section 1001 (this group control IP packet is henceforth called a balking command). And the own address and an own host name are set to the IP address storing section 1002 and the host name storing section 1003, respectively.
[0094]
The group information update process section 3500 performs the group information update process of updating the contents of the group managed table 600, or copying it to a memory card.
[0095]
In this operation gestalt, in order to raise security, the group key used within a group serves as a setup updated for every predetermined period. When the key expiration date of the group managed table 600 carries out the time-out of the group information update process section 3500, it generates a new group key.
[0096]
Here, a different key expiration date is set as group managed table 600 generate time for every node. concrete -- a predetermined expiration date, for example, double sign 30%, -- it is set as each node by making into a key expiration date the value acquired

by adding or subtracting the random value of a between at the key expiration date. For this reason, it is generated to the timing from which the time-out of a key expiration date differs by each node, the node which updates a key becomes settled in one, and it can avoid that a group's member generates a group key to coincidence.
[0097]
And it enciphers with the group key before updating the updated group key, and sends to each node which belongs to a group from the member which updated the group key. At this time, you may reset the key expiration date of each node with renewal of a key.
[0098]
Moreover, the group information update process section 3500 updates the IP address in a related database, when the IP address of each node 100 belonging to a group is updated, while updating the information on the group key which self holds, when the updated group key is received from other nodes.
[0099]
Here, with this operation gestalt, since renewal of a group's key is performed as mentioned above, it is not reflected in the group managed table 600 in the memory card used for group participating processing. Similarly, balking processing from an above-mentioned group is performed using an empty memory card, and the notice to other nodes 100 which constitute a group from a node 100 from which it seceded is performed by IPsec communication link. For this reason, modification of the group configuration member by group balking is not reflected in the group managed table 600 in the memory card used for group participating processing, either.
[0100]
For this reason, with this operation gestalt, the group information update process section 3500 also performs an update process of the group managed table 600 in a memory card.
[0101]
An update process of the group managed table 600 in the memory card which the group information update process section 3500 performs is performed when a control section 3100 judges that the group managed table 600 exists also in the memory card inserted also in the own access polish database 308.
[0102]
The group information update process section 3500 copies the information on the group managed table 600 stored in the access polish database 308 of the node 100 concerned to the group managed table 600 in a memory card.
[0103]
With this operation gestalt, in actual group participating processing, when performing group participating processing, a memory card is inserted in the node 100 which has already belonged to the group, and it is determined that a procedure performs beforehand processing which makes the newest thing the group managed table 600 in

a memory card.
[0104]
The group control IP packet reception section 3600 performs processing at the time of receiving the above-mentioned group control IP packet.
[0105]
When a subscription command is received, the IP address and host name which are stored in the IP address storing section 1002 and the host name storing section 1003 are added to the own group member managed group managed table 600 and 800, and, specifically, a security association required in order to perform the transmitting agency node 100 and cryptocommunication is created. On the other hand, they are deleted when a balking command is received.
[0106]
Next, the group managed table 600 and the application managed table 700 corresponding to an access control which are stored in the access polish database 308, and the group member managed table 800 are explained below.
[0107]
The group managed table 600 is a table which stores the information on the key shared between the information and the group for identifying the node 100 belonging to a group. The example is shown in drawing 8 .
[0108]
As shown in this Fig., the group managed table 600 The group identification descriptor storing field 601 which stores the group identification descriptor for identifying the group constituted by the node 100 connected to the network, The group key storing field 602 which stores a group key, and the group key expiration date storing field 603 which stores the expiration date of the group key, The IPsec classification storing field 604 which stores the classification of the function of IPsec used for a communication link within groups, such as AH and ESP, It has the algorithm storing field 605 which stores the algorithm used for authentication or a code, and the host name storing field 606 (606A-606B) which stores the host name which is the information which identifies the node 100 belonging to a group.
[0109]
The application managed table 700 for an access control is a table on which the information used for the access control to each application mounted in the node 100 is stored, when application with the available node 100 besides a group is mounted in the node 100.
[0110]
In addition, this table is unnecessary when only application which a node 100 offers only to access out of a group is mounted.
[0111]
An example of the application managed table 700 for an access control is shown in drawing 9 .

[0112]
As shown in this Fig., the application managed table 700 for an access control is equipped with the port number storing field 701 (701A, 701B) which stores the port number which the application wide opened by the node 100 besides a group uses. Each node 100 judges whether the application with which the IP packet concerned is going to access with reference to this table at the time of IP packet reception is the application wide opened by the node 100 besides a group.
[0113]
Next, the group member managed table 800 is explained. In order to perform IP packet communication between each node 100 based on IPv6, it is necessary to get to know the IP address of each node 100. The IP address of each node 100 belonging to a group is ICMP (Internet Control Message Protocol) from the host name of each node 100 acquired at the time of group participation. Echo By the exchange of a Request/Reply packet, it acquires by solving the address. Thus, the group member managed table 800 solves and creates an IP address from a host name in each node, and correspondence with the host name of each node 100 and IP address belonging to a group is stored there.
[0114]
An example of the group member managed table 800 is shown in drawing 10 .
[0115]
This table is equipped with the host name storing field 801 which stores the host name which specifies a node, the IP address storing field 802 which is made to correspond with a host name and stores the IP address of each node 100, and the expiration date storing field 802 which stores the expiration date of an IP address as shown in this Fig.
[0116]
When a node 100 reboots, the IP address of a node 100 may change. Moreover, if the IP address and transmission and reception which are stored in fixed time amount at the IP address storing section 802 are not performed, an expiration date may go out.
[0117]
When transmitting an IP packet to such a node, the IPv6 transmitting pretreatment section 305 of a node 100 is ICMP. Echo By the exchange of a Request/Reply packet, the address is again solved from a host name and it notifies to the group management processing section 302. In response to it, the group information update process section 3500 of the group management processing section 302 updates the security association used for the communication link in this table on which the IP address is registered, and a group.
[0118]
Next, the security association 900 stored in the SA database 309 is explained. When managing the information which should be shared in order to perform the communication link in accordance with IPsec and communicating [for example,]

between node 100A and node 100B, it is necessary to the communication link of the direction of node 100A, and both to set up the security association 900 independently from the communication link of the direction of node 100B and node 100B from node 100A.

[0119]

An example of the security association 900 is shown in drawing 11 .

[0120]

As shown in this Fig., the security association 900 contains the expiration date of assignment in a transport mode or tunnel mode, cryptographic algorithm, a cryptographic key, an authentication algorithm, an authentication key, and a key etc. as authentication or assignment of a code, and code range as SPI (security policy identifier) which identifies each security association, a transmitting agency IP address, the transmission place address, and a protocol.

[0121]

When creating the security association 900 for transmission with this operation gestalt in creating the security association 900 in each node 100 In a transmitting agency IP address, the IP address of the own node 100 for a transmission place IP address When setting up the IP address of a communications-partner point node and creating the object for reception, the IP address of the communications-partner point is set to a transmitting agency IP address, and the IP address of the own node 100 is set to a transmission place IP address.

[0122]

The group identification descriptor by which the object for transmission and the object for reception are stored in the group identification descriptor storing section 601 of the group managed table 600 is stored in SPI. Moreover, that by which the object for transmission and the object for reception are stored in the group managed table 600 at the protocol, the authentication key algorithm, the authentication key, and the expiration date, respectively is set up.

[0123]

In the above, each function of the node 100 in this operation gestalt etc. was explained.

[0124]

Next, between each node 100 in this operation gestalt connected to the network 110, a group is generated and the procedure which participates, the procedure of seceding from the group who once participated, etc. are explained.

[0125]

The case where use a transport mode as the mode and SHA-1 (it specifies as Secure Hash Algorithm 1:SHS(Secure Hash Standard) FIPS 180) is used for below for AH as an authentication algorithm as a functional classification of IPsec is mentioned as an example, and is explained. A setup of an IPsec communication link is not restricted to these.

[0126]
Moreover, in this operation gestalt, as mentioned above, a group's generation, participation, balking, renewal of information, etc. are performed using two memory cards of the memory card which stores a group's information, and the empty memory card used in case it secedes from a group.
[0127]
The group management procedure 3020 which the group management processing section 302 performs to drawing 12 is shown.
[0128]
The group management procedure 3020 is started taking advantage of a user inserting a memory card in the record-medium interface 206 of each node 100.
[0129]
And when it detects that the memory card was inserted in the record-medium interface 206, the storage interface processing section 318 of a node 100 turns on LED Wright with whom the storage interface 206 is equipped, and shows to a user that a memory card is under use.
[0130]
By having switched off LED Wright, a user can know that processing was completed and can take out a memory card.
[0131]
Moreover, the storage interface processing section 318 notifies having detected the memory card to the group management processing section 302. In response to the notice, the group management processing section 302 starts the group management processing 1000.
[0132]
First, the control section 3100 of the group management processing section 302 accesses the own access polish database 308 and the memory card by which memory card insertion was carried out through the record-medium interface processing section 318, and checks the existence of the group managed table 600 (step 3021).
[0133]
When there is no group managed table 600 in both, the group itself does not exist, namely, it judges that it is necessary to generate a group, and a control section 3100 makes the group generation processing 3210 perform in the group generation processing section 3200 here (step 3022). If the group generation processing 3210 is completed, to the storage interface processing section 318, a control section 302 will notify write-in termination of a memory card (step 3027), and will finish processing. If a control section 3100 judges that self tends to participate in the group who exists in a memory card, and makes the group participating processing 3310 perform in the group participating processing section 3300 (step 3023) and group participating processing is completed when there is nothing in the own access polish database 302 and it exists in a memory card, it will progress to step 3027.

[0134]
When there is nothing to a memory card and it exists in the own access polish database 302, if a control section 3100 judges it as what performs group balking processing by having inserted the memory card of a null although self already belongs to the group, the group balking processing 3410 is made to perform in the group balking processing section 3400 (step 3026) and group balking processing is completed, it will progress to step 3027.
[0135]
When the group managed table 600 exists in both, a control section 3100 first compares the group identification descriptor of the group managed table 600 in the access polish database 302, and the group managed table 600 in a memory card (step 3024).
[0136]
Here, if both are the same, will judge it as what performs processing which updates group information of a memory card, the processing which copies the group managed table 600 in the access polish database 302 to the group information update process section 3500 as group information update process 3510 at a memory card will be made to perform (step 3025) and the processing concerned will be completed, it will progress to step 3027.
[0137]
In step 3024, when both differ, a control section 3100 judges that the mistaken memory card was inserted, and progresses to step 3027 as it is.
[0138]
Next, the procedure of the group generation processing 1200, the group participating processing 1300, the group balking processing 1600, and the group information update process 1500 is explained.
[0139]
First, the procedure of the group generation processing 3210 is shown in drawing 13 .
[0140]
If directions of processing initiation are received from a control section 3100, the group generation processing section 3200 will generate a group key (step 3211), will generate the group identification descriptor for identifying a group (step 3212), will choose authentication (AH) as authentication and code mode (step 3213), and will choose SHA-1 as an algorithm (step 3214).
[0141]
And each is stored in the group key storing field 602, the group identification descriptor storing field 601, the IPsec classification storing field 604, and the algorithm storing field 605, and the group managed table 600 is created (step 3215). And the host name of the self-node 100 is registered into the host name storing field 606 (step 3216).
[0142]

Completion of the group managed table 600 notifies that memorized in the access polish database 308 of the self-node 100 (steps 3217 and 3218), and processing was completed while the group generation processing section 3200 copied this table to the memory card to a control section 3100.

[0143]

Next, the procedure of the group participating processing 3310 is shown in drawing 14 .

[0144]

If directions of processing initiation are received from a control section 3100, the group participating processing section 3300 will add the host name of the self-node 100 to the host name storing field 606 of the group managed table 600 on a memory card (step 3311), and will memorize the group managed table 600 on a memory card in the own access polish database 308 (step 3312).

[0145]

Next, notice processing 3710 of a new member which notifies own participation to each node 100 which creates the group member managed table 800, and which both already belongs to the group is performed (step 3313).

[0146]

And the security association 900 used for the IPsec communication link with each node 100 is generated using the information on the group managed table 600 recorded at the old step, and the information on the group member managed table 800 (step 3314), and it notifies that processing was completed to a control section 3100.

[0147]

Here, the procedure is explained about the notice processing 3710 of a new member. The procedure is shown in drawing 15 .

[0148]

It is ICMP to order for every host stored in the host name field 606 in the group managed table 600 in the notice processing 3710 of a new member. Echo Request / The IP address which acquired the IP address by Reply (step 3712), and was acquired for every host name on the group member managed table 800 is registered (step 3713).

[0149]

A subscription command is generated to the IP address of each node 100 which constitutes a group acquired at the above-mentioned step (step 3714), and it is transmitted (step 3715).

[0150]

And the following host name is read and processing of steps 1330-1360 is repeated (step 3316). Here, when the read host name is an own host name, nothing is processed but the following host name is read (step 3711). And after finishing the above processing to all the nodes except the own node 100 stored in the host name storing field 606 of the group managed table 600 (step 3717), the notice processing

1330 of a new member into a group is finished.
[0151]
In the above, the group participating processing 3310 was explained.
[0152]
Next, the group balking processing 3410 is explained using drawing 16 .
[0153]
If directions of processing initiation are received from a control section 3100, the group balking processing section 3400 will read in order the host name registered into the host name storing section 606 of the group managed table 600 in a node 100 (step 3311).
[0154]
Here, when the read host name is in agreement with a self-host name, the following host name is read.
[0155]
When the read host name is not in agreement with a self-host name, the IP address corresponding to the host name read from the group member managed table 800 is searched (step 3312). Henceforth, it is called the IP address which searched this IP address.
[0156]
Next, the balking command made into the IP address which searched the transmission place IP address is created (step 3313), and it transmits to the node 100 which has the transmission place IP address (step 3314).
[0157]
The group balking processing section 3400 deletes the data concerning the searched IP address which performed the above actuation from the group member managed table 800 which self holds (step 3315).
[0158]
Next, a thing with a transmission place IP address equal to the IP address searched from the security association 900 memorized by the SA database 309 is extracted, and the security association 900 is deleted (step 3316).
[0159]
Moreover, the security association 900 with a transmitting agency IP address equal to the searched IP address is extracted, and it is deleted (step 3317).
[0160]
After the group balking processing section 3400 performs processing of the above step 3311 – step 3317 to all the host names registered into the group managed table 600 (step 3318), it deletes the group managed table 600 which self holds (step 3319), and ends the group balking processing 3310. And processing termination is notified to a control section 3100.
[0161]
Next, the processing by the side of each node 100 at the time of [which received the

subscription command and the balking command, respectively] being transmitted in step 3715 of the notice processing 3710 of a new member into the group in the above-mentioned group participating processing 3310 and step 3314 of the group balking processing 3310 is explained below.

[0162]

This processing is performed by the group control IP packet reception section 3600, and it is called the group control IP packet reception 3610. The procedure of this processing is shown in drawing 17 .

[0163]

Each node 100 which constitutes a group will be delivered to the group control IP packet reception section 3600 of the group management processing section 302 through the IP receive section 314 and the TCP/UDP reception section 315, if a group control IP packet is received in the network interface reception section 310.

[0164]

The group control IP packet reception section 3600 which received checks whether the command identifier set as the command identifier storing section 1001 is subscription (step 3611).

[0165]

When it is (00) hex a command identifier indicates subscription to be at step 3611 (i.e., when a subscription command is received), it progresses to step 3612 and the host name of the node 100 which has transmitted the subscription command set as the host name 1003 of a group control IP packet is registered into the group managed table 600 (step 3612).

[0166]

And the host name of the node 100 which has transmitted the subscription command to the group member managed table 800, and its IP address set as the IP address storing section 1002 of a group control IP packet are registered (step 3613).

[0167]

Next, the group control IP packet reception section 3600 performs transmission of the node 100 direction of own, and processing which creates each security association 900 from the node 100 which has transmitted, transmission and the object for reception, i.e., the subscription command, of the object for transmission, i.e., node 100 direction which has transmitted the subscription command from the own node 100, and which joined newly, and which joined newly (steps 3614 and 3615).

[0168]

Next, when it is (01) hex a command identifier indicates balking to be at step 3611 (i.e., when a balking command is received), the group control IP packet reception section 3600 progresses to step 3616.

[0169]

Here, the group control IP packet reception section 3600 extracts a thing with a transmission place IP address equal to the IP address stored in IP address 1002 of

the data division 1000 of a group balking command which received, and deletes the extracted security association from the security association 900 memorized by the SA database 309 (step 3616).
Next, a host name equal to the host name which deletes the data which have an IP address equal to IP address 1002 of the received balking command from the group member managed table 800 (step 3617), and is stored in the host name 1003 of a balking command which received is deleted from the group managed table 600 on the self-node 100 (step 3618).
[0170]
By performing the above procedure in all the nodes 100 in a group, the security association 900 corresponding to the node 100 which all the nodes 100 hold and from which it seceded is deleted, and the information on the node 100 from which it seceded is deleted from the group managed table 600.
[0171]
When the node 100 which constitutes a group as mentioned above has modification, such as new subscription or balking, in other nodes 100 which received the group control IP packet transmitted from the node 100 concerned, the security association and the group managed table 600 which self holds are updated.
[0172]
In the above, group control IP packet reception was explained.
[0173]
So far, group management processing of a group's generation by the group management processing section 302, participation, balking, etc. was explained.
[0174]
Next, the procedure of using application mutually is explained below within the group generated and managed in the above-mentioned procedure.
[0175]
Use of application is performed by sending and receiving an IP packet mutually. First, transmission and reception of this IP packet are explained.
[0176]
As mentioned above, beforehand, in order to perform an IPsec communication link, the required security association 900 of a setup is generated in the group management processing 302, in case a new group configuration member is added. That is, as long as it belongs to the group, the IPsec communication link is possible.
[0177]
In transmitting an IP packet, the IPsec transmitting processing section 306 extracts the security association 900 by which the IP address which searches the SA database 309 and corresponds is stored in the key as a transmission place IP address in the transmission place IP address of IP header to transmit. Based on the information registered into the extracted security association 900, IPsec processing is performed, IPv6 transmitting after treatment 307 is performed, and an IP packet is

transmitted to a transmission place node through the network interface transmitting processing section.
[0178]
Next, the procedure at the time of IP packet reception is explained using drawing 18 .
[0179]
If an IP packet is received through the network interface reception section 310, the IPv6 reception pretreatment section 311 will check the existence of AH header in IP header which performed IPv6 reception pretreatment (step 4010) and was received (step 4020).
[0180]
If it judges that the AH header 401 is in received IP header, the IP packet will be delivered to the IPsec reception section 312.
[0181]
The received IPsec reception section 312 performs IPsec reception 3120 mentioned later (step 4030), and delivers an IP packet to the IPv6 receiving after-treatment section 313.
[0182]
And the IPv6 receiving after-treatment section 313 performs IPv6 receiving after treatment 3130 (step 4040), and ends processing.
[0183]
In addition, the IPv6 receiving after-treatment section 313 delivers the packet which finished the IPv6 receiving after treatment 3130 and which received to the TCP/UDP reception section 315 here. The received TCP/UDP reception section 315 performs reception of the received packet, and passes it to application 301 as received data.
[0184]
When it is judged at step 4020 that there is no above-mentioned header, the IP packet is delivered to the receiving access-control section 316.
[0185]
The received receiving access-control section 316 confirms whether it is an ICMP packet (step 4050).
[0186]
At step 4050, if the IP packet which received is judged to be an ICMP packet, it will deliver to the IPv6 receiving after-treatment section 313 as it is, will perform IPv6 receiving after treatment 3130 (step 4040), and will end processing.
[0187]
At step 4050, if it is judged that it is not an ICMP packet, the receiving access-control section 316 will judge that it is the IP packet outside a group to which the IP packet was transmitted from the node 100 besides a group, will perform IP packet reception 3160 outside a group mentioned later (step 4060), and will end processing.
[0188]
Next, the above-mentioned IPsec processing 3120 is explained.

[0189]
The IPsec processing section 312 will extract the transmitting agency IP address of IP header, a transmission place IP address, and the security association 900 whose SPI set as the AH header 401 corresponds from the SA database 309, if the IP packet which has AH header is received.
[0190]
And the authentication information on the IP packet which received using the authentication key memorized by the extracted security association 900 is created, and it compares with the authentication information set as the AH header 401.
[0191]
If both are in agreement, it will consider that the IP packet which received is transmission from the just node 100 belonging to a group, and will deliver to the IPv6 receiving after-treatment section 313. and the case of not being in agreement -- the -- IP packet cancellation is carried out.
[0192]
The IPsec processing 3120 was explained above.
[0193]
Next, the packet reception 3160 outside a group by the receiving access-control section 316 is explained.
[0194]
As mentioned above, in this operation gestalt, the node 100 belonging to a group has eliminated that the IP packet concerned reaches application 301 through the IPv6 receiving after-treatment section 313 and the TCP/UDP reception section 315 in the IPv6 reception pretreatment section 311, when the IP packet which does not have AH header in the IPsec communications processing section 312 when the IP packet which has AH header is received from the node 100 besides a group is received.
[0195]
However, in this operation gestalt, there are some which have opened use of the application to hold wide also to the node 100 besides a group depending on the node 100. As mentioned above, the node 100 which has such application has managed the port number for every application in the application managed table 700 for an access control.
[0196]
Since the IP packet was not able to be decoded when the IP packet which has AH header from the node 100 besides a group is received, it explained previously canceling in the IPsec communications processing section 312.
[0197]
When the IP packet reception 3160 outside a group receives the usual IP packet from the node 100 besides a group, it is processing which sends the IP packet concerned to the application wide opened to the node 100 besides a group.
[0198]

In the IP packet reception 3160 outside a group, when the node 100 which received the IP packet does not offer a service function at all to the node 100 besides a group, the IP packet which stored the access error as data is transmitted to a transmitting agency, and the IP packet which received cancels. On the other hand, when offering a certain service function to the node 100 besides a group, according to registration of the application managed table 700 for an access control, it is controlling to offer application.

[0199]

Drawing 19 is used for below and the procedure is explained to it.

[0200]

The receiving access-control section 316 performs the comparison with the transmission place port number read in the IP packet concerned, and the port number 701 registered into the application managed table 700 for an access control, when the IP packet which is not an ICMP packet is received from the IPv6 reception pretreatment section 311 (step 3161).

[0201]

Since the port number of the application with which use is permitted to the node besides a group is registered into the application managed table 700 for an access control, when both are in agreement, the requiring agency node 100 can be provided with a service function.

[0202]

In this case, the IP packet which the receiving access-control section 316 received is delivered to the IPv6 receiving after-treatment section 313, and the received IPv6 receiving after-treatment section 313 performs IPv6 receiving after treatment 3130 (step 3164).

[0203]

And the TCP/UDP reception section 315 which received the IP packet processed from the IPv6 receiving after-treatment section 313 delivers it to application 301.

[0204]

In step 3161, since there is no service function which can be offered when a port number is not in agreement, the receiving access-control section 316 generates the IP packet which stored the access error as data, transmits to a transmitting agency from the IP transmitting section 304 (step 3162), and cancels the IP packet which received (step 3163).

[0205]

In the above, the IP packet reception outside a group was explained.

[0206]

Thus, in this operation gestalt, the access permission of group inside and outside is controllable by performing an IPsec communication link and performing the communication link by the IP packet usual in the node 100 besides a group for every application according to the port number of each application managed on the

application managed table 700 for an access control between the nodes 100 in a group. Thereby, the service function used only into a group in one node 100 and the service function which everyone can use are mounted, and the access control through which it passes, respectively is made possible.

[0207]

According to this operation gestalt, it distributes to each node 100 which permits that a user uses mutually information required for the IPsec communication link containing the group key created in the node 100 which constitutes a home network through a common memory card.

[0208]

The distributed node 100 notifies having newly joined to other nodes 100 which belong to the group while setting up the security association 900 so that an IPsec communication link can be performed with other nodes 100 which belong to the group.

[0209]

The node 100 which received the notice sets up the security association 900 so that the IPsec communication link with the node 100 which joined newly, respectively can be performed.

[0210]

As mentioned above, it has realized that the device which constitutes the group generates easily the group who can perform a communication link that it can attest and safe mutually, without minding any equipments other than the device which constitutes a group called the equipment equipped with the authentication server or the key management tool when starting a communication link, and manages him with this operation gestalt, for example.

[0211]

Moreover, it has realized giving giving information required in order to generate and manage a group to each node through a storage called a memory card and a group's generation, the participation to a group, and directions of balking from a group to each node.

[0212]

Thus, the environment in which an IPsec communication link is possible can be easily built only between the devices which constitute a group, without [without it prepares special devices, such as a server, with this operation gestalt, and] making prior preparations of setting to each device which prepares the IC card equipped with two or more master keys etc., and constitutes a group beforehand.

[0213]

Moreover, with this operation gestalt, also when application which can use only the node in a group for one node, and application which can also use the node besides a group are mounted, each access control can be realized easily.

[0214]

In addition, although the memory card was mentioned as the example and this

operation gestalt explained it as a storage used in case the directions at the time of group generation, subscription, and balking are performed, the storage to be used is not restricted to this. It may be the storage of a portable mold, and as long as each node is equipped with the interface, you may be what kind of storage.

[0215]

Moreover, although considered as a setup of delivering and receiving information required in order to perform an IPsec communication link with a storage, with this operation gestalt, it is not restricted to this. For example, each node is equipped with an input unit and a user may be made to input.

[0216]

Furthermore, although the input of an empty memory card was mentioned as the example and explained as a cause which starts the balking processing from a group, it is not restricted to this. For example, each node is equipped with a reset button and a user may be made to give the directions which start balking processing through the reset button.

[0217]

Moreover, it has realized notifying termination of group generation and subscription processing to a user by having LED. The function for a notice is not restricted to this, either.

[0218]

In addition, this invention is not limited to the above-mentioned operation gestalt, and various deformation is possible for it within the limits of the summary.

[0219]

For example, with the above-mentioned operation gestalt, although explained taking the case of the network in **, this invention is not limited to this. This invention is widely applicable to various network systems which need authentication mutually.

[0220]

Next, the operation gestalt of the subgroup which restricts the node which can be used for user correspondence in a group by Node F from the node A which is a candidate for use in the range which the manager of a node recognizes based on the operation gestalt mentioned above is explained with reference to drawing 31 from drawing 20 .

[0221]

Drawing 20 shows the example of 1 configuration of the network in ** which applied this invention, the small office network called SOHO, and a local network which makes the floor network of office representation. This invention explains hereafter the case where this invention is applied in **, as an example. The network in ** consists of PCs, such as AV equipments, such as household-electric-appliances devices, such as two or more nodes 105 (105 A, B) and 106 (106 C-F), for example, a microwave oven, and an air-conditioner, television, and video, and a sensor, and each device enables transmission and reception of an IP packet by IPv6. This network realizes service

provision to the actuation from nodes 105 and 106 and the other nodes 105 and 106 of the service function with which each is equipped, or the other nodes 105 and 106.
[0222]
Moreover, based on an above-mentioned operation gestalt, SA900 which can IPsec communicate using the group key 602 common to a group is set as each node, and the nodes 105 and 106 of these plurality will be in the condition that the IPsec communication link which used said group key 602 for the communication link between groups can be performed. Hereafter, this group is called the root group 107. Construction of the root group 107 sets up the root group's 107 SA900 for transmission and SA900 for reception to all the nodes 105 and 106 in all the nodes 105 and 106 that constitute the root group 107 on the group managed table 600 on the group access database 308, and the SA database 309. In addition, suppose that encryption by 3DES is applied with this operation gestalt in the IPsec communication link used for the communication link between groups in a root group.
[0223]
With this operation gestalt, the user interface function with which a node is equipped divides a network device roughly into two. The first node 105 is the interface function with which PC is equipped, for example, the display which can display the host name list of the nodes which constitute the network in **, and a node equipped with the keyboard in which an alphabetic character input is possible. The second node 106 is a node equipped with the minimum interface for operating the function with which a node is originally equipped. As a device equivalent to the first node 105, PC, television, household-electric-appliances control remote control, etc. are assumed, node A105A and node B105B are made into the first node 105 by drawing 20 , and node F106F are made into the second node from node C106C by drawing 20 as a device equivalent to the second network device 106 supposing white home appliances, a sensor, etc. which were called the air-conditioner and microwave oven.
The hardware configuration of the first node 105 is shown in drawing 21 .
[0224]
If it is one or more node proper function parts 202 with which a node 105 is equipped, for example, an air-conditioner For example, the processing section which manages an air conditioning function, a temperature function manager, timer ability, etc., The group access database 308 and the SA database 309 which realize the group communication link equipped with the program and user access control which are performed by the processor 200 which controls a network card 205, a proper function part, and a network card, and the processor The data input interface section 209 which connects a keyboard with the data output interface section 208 which connects the display for the memory 201 to memorize and a user interface, the storage interface 206 which offers the interface of memory card 207 grade, And it consists of system buses 203 which connect these. Said storage interface 206 possesses LED (light emitting diode) Wright who notifies a user of under the writing of

the storage to insert, and shows under writing or processing to a user by light of LED Wright. The hardware configuration of the second node 106 does not have the data output interface section 208 and the data input interface section 209 which are used from the hardware configuration of said first node 105 for a user interface.

[0225]

The software configuration of the first node 105 is shown in drawing 20 .

A network is minded. One or more application programs 301 which carry out service provision between group configuration equipment, the TCP / UDP transmitting processing section 303 which realizes a communication link, the IP transmitting section 304, the network interface transmitting processing section 317 which controls a network card, In order to realize the SA database 309 and group communication link which manage the network interface reception section 310, the IP receive section 311, the TCP/UDP reception section 315, and the security association (henceforth, SA) 900 of IPsec The access polish database 308 which manages the information and group information about the access control to the network device to be used, the group management processing section 302 which performs group management, the storage interface processing section 318 which controls a storage interface, And it constitutes from the data output interface section and the user interface processing section 151 which controls the data input interface section. The IP transmitting section 304 The IPsec transmitting processing section 306 which performs IPsec processing when the existence of the IPv6 transmitting pretreatment section 305 which creates IP header from DDA to Pseudo which the TCP/UDP transmitting processing section 303 created, and SA900 is investigated and there is SA900, It consists of the IPv6 transmitting after-treatment sections 307 which pass an IP packet to the network interface transmitting processing section 317. The IP receive section 314 The comparison of IP packet header to the payload length which received from the network interface reception section 310, and received-data length, The IPv6 reception pretreatment 311, AH header which process a header option, The IPsec reception section 312 which searches SA900 when there is an ESP header, and performs authentication or decode processing, AH header, When there is no ESP header, the receiving access-control section 316 which judges whether an IP packet is received, and IP header are transposed to a Pseudo header, and it constitutes from the IPv6 receiving after-treatment section 313 which passes received data to the TCP/UDP transmitting processing section 315.

[0226]

The group management processing section 302 carries out carrying out the user-access control processing 2100 in which the access-control setting demand from a user is received, and the subgroup management processing 2200 performed in the processing to the command reception about the subgroup management from other network devices based on the operation gestalt mentioned above in addition to the root group generation processing 3200, the participating processing 3300, the balking

processing 3400, the information update process 3500, and the group-control IP packet reception 3600.
[0227]
as the group access database 308 -- the group managed table 600, the access user managed table 2001, and access -- an application -- the managed table 2003 is arranged.
[0228]
SA900 of the transmitting agency address prepared as an SA database 309 for every transmit direction for realizing an IPsec communication link and receive direction and a receiving agency address mapping is arranged.
It considers as the configuration which removed the user interface control section 151 used for a user interface, and the user access control section 2100 from the software configuration of said first node 105 as a software configuration of the second node 106. In addition, the access user managed table 2001 is not arranged on the group access database 120.
Subgroup 108 configuration which applies this invention to drawing 22 is shown. By a diagram, two subgroups 108 are shown. A subgroup 108 carries out grouping of the node which can be used for user correspondence, and when realizing service whose user used other nodes 105 and 106 from the first node 105, User A can use only the nodes 105A, 105B, and 106C which constitute subgroup a108A, and it can use only the nodes 105A, 106D, and 106E from which User B constitutes subgroup b108B. User B cannot use the service which accesses node C106C from node A105A.
[0229]
In a home network, if father's subgroup is constituted from PC, television, an air-conditioner, and video by setting up a subgroup 108 on the root group 107, a temperature setup of an air-conditioner and a reservation setup of video can be performed from PC and television. On the other hand, although a son can do a video reservation setup from television by constituting television and video as a son's subgroup, control that a temperature setup of an air-conditioner cannot be performed is attained.
[0230]
Hereafter, the construction approach of this subgroup 108 and operations sequence are explained using drawing 31 from drawing 23 .
Drawing 23 shows three phases at the time of the network connection in one nodes 105 and 106. The first phase is the group-less phase 2301 which is in the condition which connected nodes 105 and 106 with the network. It sets group-less phase 2301 and the root group phase 2302 which is the second phase comes based on said operation gestalt by subscription in root group 107 generation and the root group 107 of a node 105,106. Suppose that cryptocommunication by 3DES using the common group key 602 is performed within the root group 107 in this second phase in the node 105 in the root group 107, and the communication link between 106. In the root

group 107, the subgroup phase 2303 which is the third phase comes by a user's access privilege and node selection which can be used. In the third phase, cryptocommunication of 3DES using the common group key 602 is performed within a subgroup 108 in the node 105 in a subgroup 108, and the communication link between 106.

Drawing 24 is drawing showing the procedure of the user access control processing 2100 in which user access control in the group management processing section 302 is performed. In order to receive the demand from a user, the user access control processing 2100 is started in the first node 105. When a user may start this processing and it participates in the root group 107, it may start this processing and may be operated as a resident program of a node 105. The user access control processing 2100 can be started at root group phase 2302 or subgroup phase 2303:00 (step 2101).

I display "a right setup of user access", "right disconnection of user access", and "service use" on a display (step 2102), and have what is used for a user chosen, and right setting processing (2110) of user access, right release processing (2130) of user access, and subgroup access privilege check processing (2150) are performed by selection.

Drawing 25 shows the procedure of the right setting processing 2110 of user access. The host name registered into the group managed table 600 to the root group 107 who has managed in the group access database 308 as the 1st step is displayed on a display (step 2111). The group managed table to the root group 107 presupposes that the root is set as the area of classification 607.

Two or more host names to register as the 2nd step as a subgroup 108 which the user inputted are received, on the group access database 308, the new group managed table 600 is allocated, classification 607 is made into a factice, and a host name is registered (step 2112).

As the 3rd step, the group identification descriptor 601 of other group managed tables 600 and the conflicting group identification descriptor 601 are chosen, and a group identification descriptor 501 is set as the new group managed table 600 (step 2113).

As the 4th step, the common group key 602 for codes is generated by the subgroup 108, it is set as the new group managed table 600, and a key shelf-life and 3DES are set up as cryptographic algorithm (step 2114).

As the 5th step, to all the network devices 105B and 106C that constitute a subgroup 108, the subgroup creation demand frame 2601 is created and it transmits (step 2115).

[0231]

It constitutes from the command identifier which shows a subgroup creation demand for a transmitting frame structure as shown in drawing 26 , the group identification descriptor 601 of a subgroup, a host name list of all the nodes that constitute a group, a group key 602 of a subgroup, and its expiration date. It is transmitted as UDP datagram through the TCP/UDP transmitting processing section 303, and in the IP

transmitting section 304, it is enciphered with the root group's 107 group key, and this frame 2601 is transmitted. Transmission to each network device is checked by the check frame 2602 returned from each node. As shown in drawing 26 , the check frame 2602 consists of the command identifiers and group identification descriptors 601 which show the confirmation of receipt. When the fixed time amount and check frame 2602 cannot be received, the subgroup creation demand frame 2602 may be resent. In case the subgroup creation demand frame 2601 is transmitted, the resolver demand containing the host name which obtains an IP address from the host name of nodes 105 and 106 is told to the IP transmitting section 310. The resolver table constituted from a host name with which IP transmitting section was equipped 310, an IP address, and a timer which manages table registration time amount is searched, the IP address which is in agreement with a host name is searched, and it considers as the returned value over a demand. It is ICMP when there is no host name which corresponds in a table. Echo While solving the address from a host name and registering the group of a host name and an IP address into a resolver table from Rquest/Reply, it considers as the returned value over a demand.

[0232]

As the 6th step, SA900 and SA900 for reception for transmission to all the network devices that constitute a subgroup 108 are created (step 2116).

The configuration of SA900A is shown in drawing 27 .

[0233]

As SA900A for transmission, a group identification descriptor 601 is set up as an SPI, the address of a self-network device is set up as a transmitting agency IP address, a subgroup is constituted as a transmission place IP address, and also the IP address of a network device is set up. this operation gestalt -- setting up ESP as a protocol, the mode sets up transport, and cryptographic algorithm sets up the group key 601 of a subgroup as 3DES and a cryptographic key. As SA900A for reception, it is the same configuration as SA900 for transmission except setting up the IP address of another network device as a transmitting agency IP address, and setting up the address of a self-network device as a transmission place IP address.

[0234]

As the 7th step, the access user ID and the password by the user are received through the data input interface section 209 and the data output interface section 208 (step 2117).

[0235]

The authentication key 2002 is generated as the 8th step (step 2118).

[0236]

The global IP address of user ID, a password, the authentication key 2002, and a self-network device and the group identification descriptor 601 of a subgroup are written in on the memory card [finishing / a format of the empty which the user inserted / as the 9th step] 207 (step 2119).

[0237]
As the 10th step, the group identification descriptor of the authentication key 2002, user ID, and a subgroup is set as the access user managed table 2001 of the group access database 308 (step 2120).
[0238]
As the 11th step which is the last of the right setting processing 2110 of user access, to all the nodes that constitute a subgroup 108, the subgroup access privilege setting frame 2603 is created, and it transmits (step 2121).
[0239]
A transmitting frame structure is constituted from the command identifier which shows a subgroup access privilege setup as shown in drawing 26 , the group identification descriptor 601 of a subgroup, user ID, an authentication key 2002, and a password, and the same procedure as the subgroup setting demand frame 701 mentioned above performs transmission and a transmitting check.
[0240]
Next, the procedure performed by the subgroup management processing 2200 in the group management processing section 302 in the nodes 105 and 106 which constitute 108 in the subgroup which received the subgroup setting demand frame 2601 and the subgroup access privilege setting frame 2603 is shown in drawing 28 .
[0241]
The subgroup setting processing 2200 can be started at root group phase 2301 or subgroup phase 2303:00 (step 2201).
When the subgroup setting demand frame 2601 is received, the group managed table 600 is allocated and the information which a frame has is set up. Next, SA900 for transmission and SA900 for reception are created as the right setting processing 2110 of user access showed (step 2202).
[0242]
When the subgroup access privilege setting frame 2603 is received and a self-node is the first node 105, the access user managed table 2001 of the group access database 308 is allocated, and the group identification descriptor which is the information which a frame has, user ID, an authentication key, and a password are set up (step 2203).
The confirmation-of-receipt frame 2602 shown in drawing 26 is returned as the confirmation of receipt of the subgroup setting demand frame 2601 and the subgroup access privilege setting frame 2603 (step 2203).
[0243]
Construction of a subgroup is completed by the above.
[0244]
Next, the procedure of the subgroup access privilege disconnection processing 2150 is shown.
When a manager or a user chooses subgroup access privilege disconnection, it transmits to all the network devices that carry out the subgroup configuration of the

subgroup release request frame 2604 which is shown in drawing 26 , and which is constituted from a command identifier which shows a subgroup release request, and a group identification descriptor 601 of a subgroup. Then, the group managed table 600, access, and a security association with the group identification descriptor 601 of the subgroup specified by the manager are released, and the correspondence column of the corresponding access user managed table 2001 is deleted.

[0245]

In the subgroup management processing 2200 in the group management processing section 302 which received this frame, as shown in drawing 28 , the group managed table 600 and SA900 with the subgroup identifier 601 directed by the received frame are deleted (step 2205), and when a self-node is the first node 105, the correspondence column of an access user managed table is deleted (step 2206).

[0246]

The created subgroup is releasable with the above procedure.

Hereafter, the communication procedure in a subgroup 108 is explained using drawing 31 from drawing 29 .

[0247]

A procedure in case a user uses a subgroup 108 is shown.

From the user access control processing 2100, a user chooses "service use" from "a right setup of user access", "right disconnection of user access", and "service use" which were displayed on the display (step 2102).

[0248]

When two or more services can be offered, one service may be made to choose at the time of this selection. The above-mentioned selection performs subgroup access privilege check processing 2150.

In drawing 29 , the procedure of the subgroup access privilege check processing 2150 is shown. As the 1st step, insertion of the memory card 207 which memorized user ID, the password, and the authentication key is directed to a user (step 2151).

[0249]

A user receives insertion of a memory card 207, the access user managed table 2001 on the user ID on a memory card 207 and the corresponding group access database 308 is searched as the 2nd step, and it checks that the password which the memory card on a memory card has memorized, and the password of the access user managed table 2001 are in agreement (step 2152).

[0250]

When there is no access user managed table 121 whose user ID corresponds, or when a password is an inequality, an authentication error is displayed on a display and processing is ended (step 2153).

[0251]

As the 3rd step, the application corresponding to service specified by a user is started, and application receives the transmit-port number assigned to the socket

used for data transmission and reception (step 2154).
An assignment beam transmit-port number is set as a socket in the port number area 608 of the group managed table 600 which is in agreement with the group identification descriptor 601 on a memory card (step 2155).
[0252]
As the 4th step, a node starts the user access condition process 2300, and ends subgroup access privilege check processing (step 2156).
With this operation gestalt, in an application program 301, in order to perform data transfer, while you open a socket as initial processing, since it is assigned from the socket processing section, suppose that a transmitting agency port number can be notified to the subgroup access privilege check processing 2150.
[0253]
The procedure of the user access condition process 2300 is shown in drawing 30 .
In the user access condition process 2300, in order to detect that the user removed the memory card 207 and to end the access privilege of a subgroup 108, the transmitting agency port number set as the group managed table 600 in the group access privilege check processing 2150 is deleted (step 2301).
[0254]
It is possible for this to stop the subgroup 301 use by the user.
Next, the IP packet transceiver procedure in the subgroup by the application specified by a user is shown.
[0255]
Drawing 31 shows the procedure of the IPsec transmitting processing section 306.
As the 1st step, SA whose transmitting agency IP address and transmission place address of a transmitting packet correspond is searched from SA database (step 4101).
As the 2nd step, if the user access condition process 2300 is not starting [be / it], the classification of SA900 will search what is the root (step 4102). It judges whether you are the root group 107 by the classification 607 of the group managed table 600 with the group identification descriptor 601 of SA900 the transmitting agency IP address and whose receiving agency IP address corresponded.
[0256]
Using the group key 602 which the SA900 has managed, an IP packet is enciphered and IPsec transmitting processing is performed (step 4103).
If the user access condition process 1100 is starting, as the 3rd step, that whose classification of SA900 is a factice is searched (step 4104), it investigates whether the port number of the group managed table 122 corresponding to SPI of searched SA900 and the transmitting agency port number of the transmitting packet TCP or an UDP header are in agreement (step 4105), and when in agreement, IPsec transmitting processing 4103 will be performed using the SA900.
[0257]

Processing is ended when there is no SA in agreement. In this case, since an IP packet is transmitted without performing IPsec processing, it is canceled by the access control of a receiving side as except the communication link of a root group or a subgroup with the procedure shown below.
Next, the IPsec reception procedure at the time of receiving the IP packet which transmitted in the procedure shown in drawing 31 is shown. In the IPv6 reception pretreatment section 311 of the IP receive section 314, when AH header or an ESP header is in a receive packet, the IPsec reception section 312 is started.
[0258]
SA which is in agreement with SPI contained in AH header or an ESP header is searched with the IPsec reception section 312 from SA database. The cryptographic key contained in searched SA database performs decode processing.
[0259]
When there is not AH header or an ESP header, the port number and the transmission place port number of a receive packet which are registered into the application managed table 700 for an access control even if the IPsec communication link is not performed by the receiving access-control section 316 are compared, and when in agreement, a packet is handed over to the TCP/UDP reception section 315 which hits the high order processing section. If the other IP packets are not control packets, such as an ICMP packet, they will cancel a receiving IP packet as a packet of the outside a root group or for a subgroup.
[0260]
Although the classification of the group managed table 600 is a factice, and SA900 is specified in the IPsec transmitting processing shown in drawing 31 at the time of SA900 retrieval corresponding to a transmitting packet when the port number of the transmitting agency port number of a transmitting packet corresponds The active area which memorizes a subgroup identifier is prepared in the group access database 308. Instead of memorizing the transmitting agency port number obtained on the corresponding group managed table 600 in drawing 29 at the time of application starting (steps 2154 and 2156) When the group identification descriptor 601 memorized by the memory card 207 is set as said active area and the group identification descriptor 601 of said active area and SPI of SA900 are in agreement in the IPsec transmitting processing 132, it is also possible to specify SA900.
[0261]
In this case, what is necessary is to manage only a group identification descriptor 601 in said active area, even when carrying out simultaneous operation of two or more application programs 301.
[0262]
On the other hand, when managing a port number on the group managed table 600, two or more port numbers corresponding to an application program 301 are required.
[0263]

Thus, it sets in the root group 107 who consists of nodes which perform an IPsec communication link by two or more nodes 105 and 106 equipped with the common key. The subgroup 108 constituted from two or more nodes 105 and 106 controlled from the first node 105 equipped with the user interface is constituted. So that the second common cryptographic key can realize an IPsec communication link within the subgroup 108 In the first node 105, other firsts and the second node 105 and 106 are received in the user access information memorized to the common cryptographic key and storage 207 of a subgroup at the time of a subgroup setup. It transmits using the root group's 107 cryptocommunication, and a subgroup 108 is built.

[0264]

In the nodes 105 and 106 which constitute a subgroup 107 by this When SA900 which set up the group key of a subgroup 108 is set up and a user uses from the first node 105, Put a storage 207 into a node 105 and a user's authentication and the subgroup 108 to be used are identified. In case it has a means to memorize the port number 608 of the application 301 to be used in a node 105 and transmits from a node When the transmitting agency port number which constitutes UDP or the TCP header of said port number and transmitting packet at the time of SA900 retrieval is in agreement in IPsec transmitting processing, by transmitting using the SA900 The communication link only in a subgroup 108 and the user access control to a group are realizable.

[0265]

Next, the procedure in which the user who had the access privilege to the subgroup from an external network using drawing 36 from drawing 32 realizes access to a subgroup is shown.

Drawing 32 is drawing showing an example of the system configuration of this operation gestalt.

[0266]

Constituting from a host 4201 linked to the network in ** and an external network, and an external network, and nodes 105A, 106B, 106C, and 106D which constitute the network in **, these nodes 105 and 106 constitute the root group 107. With this configuration, node A105A considers as the first node equipped with the user interface, and presupposes that the subgroup 108 constituted from node A105A, node B106B, and node C106C is built according to the procedure of the operation gestalt mentioned above.

[0267]

A user with the access privilege to a subgroup 108 has the memory card 207 which stores user ID, the password, the authentication key, etc., and shows the procedure which accesses a subgroup 108 from a host 3201.

[0268]

It carries out [having mounted beforehand software which performs subgroup access client processing 4301 for realizing the access control to a subgroup on the host 4201,

and], and suppose that it is started by the user.
[0269]
The procedure of the subgroup client processing 4301 is shown in drawing 33 .
As the 1st step, 207 insertion directions of said memory card and the input of user ID and a password are directed by display display to a user (step 4302).
[0270]
In response to insertion of a memory card 207, and the input of the user ID from a user, and a password, it checks that the user ID, password, and input value on a memory card 207 are in agreement as the 2nd step (step 4303).
When not in agreement, a user authentication error is displayed and processing is ended (step 4304).
[0271]
When in agreement, the IP address memorized to the memory card 207 is transmitted as the transmission place address as UDP or a TCP packet as an authentication information frame 4401 which shows the authentication information which calculated user ID and a password with the authentication key 2002 to drawing 34 as the 3rd step (step 4305, step 4306).
[0272]
Suppose that 3DES of the cryptographic algorithm which is a common key encryption system is used about said operation.
[0273]
It waits for reception of the authentication acceptance frame 4402 shown in drawing 34 returned by node A105A to the authentication information frame 4401 as the 4th step (step 4307).
[0274]
If the State is O.K. as the 5th step when a frame is received, the authentication group key information which a frame has will be decrypted with the authentication key 126 on a memory card, and the group key 124 of a subgroup will come to hand (step 4308).
If the State is NG, a user authentication error will be displayed on a display and processing will be ended (step 4304).
[0275]
SA900 for transmission and SA900 for reception which set up the group key 124 of the subgroup 301 which made the IP address on a memory card 207 the transmitting agency / transmission place as the 6th step are created (step 4310).
[0276]
Since it is sharable with the host 4201 who connected the group key 601 of the subgroup 108 of the network in ** to the external network with the above, in the communication link with node A105A which constitutes a subgroup 108, the cryptocommunication using the group key 601 of a subgroup becomes possible.
[0277]
In this client processing, the access privilege release frame 3403 shown in drawing 34

to node A105A as the 7th step is sent to node A105A noting that the access privilege to a subgroup 108 is lost, when a memory card 207 breaks away (step 4311).
[0278]
About the packet sent from a host 4201, the confirmation of receipt of a frame may be performed using the confirmation-of-receipt frame 4404 shown in drawing 34 .
As the 8th step, SA900 created at the 6th step is released (step 4312).
[0279]
The processing configuration of the group management processing section 302 in first node 105A which receives access from an external network is shown in drawing 35 .
[0280]
The group management processing section 302 consists of application proxies 2400 for starting the application program for using the network device which constitutes the subgroup from the remote access control processing 2500 for receiving access from an external network, and an external network in addition to the subgroup management processing 2200 and the user access control processing 2100.
[0281]
The procedure in the remote access control processing 2500 is shown in drawing 36 .
The remote access control processing 2500 is started when the frame from the host 4201 of an external network is received.
[0282]
Subnet PURIFIKUSU of a transmitting agency IP address can judge that it is a frame from the host 4201 of an external network from differing from subnet PURIFIKUSU assigned to the network in **.
[0283]
In the group communication link, when [in IPsec] an encryption communication link has not been carried out, in order to avoid that an IP packet is canceled in the receiving access-control section 316 since it is by the communication link from the network device besides a group, the port number of the remote access control processing 2300 is beforehand registered into the application managed table 700 for an access control. This registers the port number assigned by the initialization processing at the time of starting the group management processing section 302, or the fixed port number.
[0284]
In the case of the authentication information frame 4401 shown in drawing 34 , a receiving frame decodes frame 4401 authentication information with the authentication key 2002 which is in agreement with the group identification descriptor 601 of the subgroup of the authentication information frame 4401, and picks out user ID and a password from an access user managed table (step 2501).
[0285]
It checks that it is in agreement with the value which the access user managed table 2001 whose user ID and password of this correspond with the subgroup identifier 601

has (step 2502).
[0286]
If not in agreement, a packet is canceled, the authentication acceptance frame 4402 shown in drawing 34 which set the State to NG is returned, and processing is ended (step 2503).
When in agreement, a host 4201 is returned as an authentication acceptance frame 4402 which indicates the State to be the group key information which enciphered the group key 602 of the corresponding group managed table 600 of a subgroup 108 with the authentication key 2002 to drawing 34 set to O.K. (step 2504).
[0287]
SA900 which set up the group key 602 of the subgroup 108 which made a host's 4201 IP address the transmitting agency / transmission place is created (step 2505).
In order to enable it to use the application which node A105A offers by the host 4201, the application proxy processing 2400 is started (step 2506).
[0288]
When the access privilege release command 4403 is received from a host 4201, the check frame 4404 shown in drawing 34 is returned to a host 4201 (step 2507), SA900 between node 105A is released with a host 4201 (step 2508), the port number of the corresponding group managed table 600 is deleted (step 2509), and the application proxy processing 2400 is ended (step 2510).
[0289]
Furthermore, the group key 602 of the subgroup 108 accessed by the host 4201 is updated (step 2511).
[0290]
Thereby, a subgroup cannot be accessed though the key information on subgroup access remains in the host 4201.
[0291]
The procedure of the application proxy processing 2400 is shown in drawing 37 .
[0292]
It is operating as a Web server and suppose that application proxy processing 2400 is communicated with the HTTP base between the host 4301 linked to an external network, and node A105A. First, a subgroup 301 is constituted as application proxy processing 114.
[0293]
Next, the service application information which can be used is notified to a user as the 1st step (step 2401).
[0294]
As the 2nd step, assignment of the service application used from a user is received, and the corresponding application program 301 is started in node A105A, and it is based on the operation gestalt which mentioned the transmitting agency port number above, and receives (step 2402).

[0295]
It is the HTTP base between the 1st host 4301 in a step and the 2nd step and node A105A.
[0296]
It registers with the group managed table 600 with the group identification descriptor 601 which corresponds the transmitting agency port number which came to hand as the 3rd step (step 2403).
The application program 301 of node A105A is operated through the application proxy processing 2400 from a host 4301 (step 2404). By the application proxy, a node is substituted for the communication to application and, specifically, it is performed. The demand to other nodes 106B and 106C which constitute a subgroup 108 from an application program 301 of node A105A performs the access control of a subgroup communication link according to the IPsec transmitting procedure of drawing 31 which is the operation gestalt mentioned above.
[0297]
In the right decision processing 2110 of user access of drawing 25 moreover, as storage information on a memory card 207 Make a memory card 207 memorize the address and the host name of nodes 105 and 106 which constitute a subgroup 108, and it sets to the second node 106. The group access database 305 is made to create the access user managed table 2001 at the time of subgroup bitter taste access privilege decision frame 2603 reception. In the group management processing section 302 shown in drawing 35 , like the first node 105 and by performing the remote access control processing 2500 and application proxy processing 2400 In a host 4301, when a user chooses the host name memorized by the memory card 207, it becomes possible to carry out direct access to all the nodes 105A, 106B, and 106C that constitute a subgroup 108.
[0298]
It can participate in the group communication link of the network in **, without arranging a special authentication server by distributing the common key of a subgroup to a host, while such procedure realizes user access authentication between the host located in an external network, and the node which built the subgroup.
[0299]
According to this operation gestalt, a user's second original group communication link is realizable by choosing the network device which a user can use, and enciphering and distributing the second common cryptographic key used by the selected network device by the aforementioned cryptographic key (the first cryptographic key) from the network device which performs said group communication link.
Moreover, while managing the second cryptographic key, the corresponding user's identifier, and the information on a password with a network device and a storage By distributing to the network device which manages the identifier of the second

cryptographic key with a storage, manages said identifier by the second cryptographic key and the pair by the network device, enciphers said information by the first cryptographic key, and performs other second group communication link In case a user uses a network device, it sets to any network device. In case it checks that the information on a storage and the information on a network device are in agreement and a user communicates, the use propriety of the user to a group communication link can be controlled by carrying out the group communication link by cryptocommunication by the second common cryptographic key which becomes the identifier of a storage, and a pair.

[0300]

Moreover, the transmitting agency port number which memorized the transmitting agency port number of the application which a user uses, and was remembered to be the transmitting agency port number of a packet at the time of packet transmission is compared, and only when in agreement, the use propriety to the group communication link by canceling, if it is not the enciphered packet can be controlled by the receiving side by performing cryptocommunication by the second common cryptographic key.

[0301]

Furthermore, with this operation gestalt, the address and the authentication key of a network device are managed with a storage. By requesting management to the network device which manages an authentication key in a network device, enciphers by the first cryptographic key, and performs other second group communication link In case a user starts the network device second for a group communication link, and a communication link from the network device which is not a candidate for a group communication link, with the authentication key of a storage Encipher the password and user ID of a storage and the encryption information is transmitted to addressing to the address of a storage. After decrypting user ID and a password with the authentication key by the network device second for a group communication link and checking user ID and a password The cryptocommunication in the second cryptographic key is realizable by enciphering and returning the second common cryptographic key with an authentication key between the network devices which are not the candidates for a group communication link.

[0302]

[Effect of the Invention]

In this operation gestalt, even if it does not hold the equipment specially equipped with the authentication server or the key management tool, between the devices which constitute a group, it attests that it is group configuration equipment mutually, and the group who realizes a safe communication link can be generated easily, and can be managed.

[0303]

Moreover, when a device has the application with which only the device in a group is provided, and the application with which the device besides a group is provided, the

access control can be performed with an easy configuration.

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the system configuration of the operation gestalt which applied this invention.

[Drawing 2] It is drawing showing the hardware configuration of the node in this operation gestalt.

[Drawing 3] It is drawing showing the software configuration in the node in this operation gestalt.

[Drawing 4] It is drawing showing the configuration of the IP packet with AH header used for a group communication link.

[Drawing 5] It is drawing showing the configuration of the IP packet with an ESP header used for a group communication link.

[Drawing 6] It is drawing showing the functional configuration of the group management processing section which can set this operation gestalt.

[Drawing 7] It is drawing showing an example of the configuration of the data division of the group control IP packet in this operation gestalt.

[Drawing 8] It is drawing showing an example of the configuration of a group managed table.

[Drawing 9] It is drawing showing an example of the configuration of the application managed table for an access control.

[Drawing 10] It is drawing showing an example of the configuration of a group member managed table.

[Drawing 11] It is drawing showing an example of the information configuration set up as a security association.

[Drawing 12] It is drawing showing the procedure of group management processing.

[Drawing 13] It is drawing showing the procedure of group generation processing.

[Drawing 14] It is drawing showing the procedure of group participating processing.

[Drawing 15] It is drawing showing the procedure of the notice processing of a new member into a group.

[Drawing 16] It is drawing showing the procedure of group balking processing.

[Drawing 17] It is drawing showing the procedure of group control IP packet reception.

[Drawing 18] It is drawing showing the procedure of IP receive section at the time of IP packet reception.

[Drawing 19] It is drawing showing the procedure of the receiving access-control section at the time of IP packet reception.

[Drawing 20] It is drawing showing the network system constituted from a software configuration of a network device, and a network device.

[Drawing 21] It is drawing showing a hardware configuration and the storage information on a storage.

[Drawing 22] It is drawing showing the range of the first group communication link and the second group communication link.

[Drawing 23] It is drawing showing the connection phase of the network device which performs a group communication link.
[Drawing 24] It is drawing showing the procedure which performs user access control in the group management processing section.
[Drawing 25] It is drawing showing **** for the procedure of the right setting processing of user access.
[Drawing 26] It is drawing showing the frame structure exchanged between the network devices which perform other group communication links by processing of the right setting processing of user access.
[Drawing 27] It is drawing showing the example of 1 configuration of SA.
[Drawing 28] It is drawing showing the subgroup management procedure in the group management processing section.
[Drawing 29] It is drawing showing the procedure of subgroup access privilege check processing.
[Drawing 30] It is drawing showing the procedure of a user access condition process.
[Drawing 31] It is drawing showing the procedure of the IPsec transmitting processing section.
[Drawing 32] It is drawing showing an example of the system configuration which applies this invention.
[Drawing 33] It is drawing showing the procedure of subgroup access client processing.
[Drawing 34] It is drawing showing the frame structure exchanged with a host between nodes.
[Drawing 35] It is drawing showing the processing configuration of the group management processing section in the first node.
[Drawing 36] It is drawing showing the procedure in remote access control processing.
[Drawing 37] It is drawing showing the procedure in application proxy processing.
[Description of Notations]
100, 105, 106 -- A node, 107 -- A root group, 108 -- Subgroup, 207 -- A memory card, 301 -- Application, 302 -- Group management processing section, 308 -- An access polish database, 309 -- SA database, 314 -- IP receive section, 304 -- IP transmitting section, 312 -- IPsec reception section, 316 -- The receiving access-control section, 600 -- A group managed table, 700 -- The application managed table for an access control, 800 -- A group member managed table, 900 -- Security association, 2001 -- An access user managed table, 2002 -- An authentication key, 2100 -- User access control processing, 2150 -- Subgroup access privilege check processing, 2200 -- Subgroup management processing, 2400 -- Application proxy processing, 2500 -- Remote access control processing, 3100 -- A control section, 3200 -- The group generation processing section, 3300 -- Group participating processing section, 3400 [-- A host, 4301 / -- Subgroup access client processing.] -- The group balking processing section, 3500 -- The group information update

process section, 3600 -- The group control IP packet reception section, 4201

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the system configuration of the operation gestalt which applied this invention.
[Drawing 2] It is drawing showing the hardware configuration of the node in this operation gestalt.
[Drawing 3] It is drawing showing the software configuration in the node in this operation gestalt.
[Drawing 4] It is drawing showing the configuration of the IP packet with AH header used for a group communication link.
[Drawing 5] It is drawing showing the configuration of the IP packet with an ESP header used for a group communication link.
[Drawing 6] It is drawing showing the functional configuration of the group management processing section which can set this operation gestalt.
[Drawing 7] It is drawing showing an example of the configuration of the data division of the group control IP packet in this operation gestalt.
[Drawing 8] It is drawing showing an example of the configuration of a group managed table.
[Drawing 9] It is drawing showing an example of the configuration of the application managed table for an access control.
[Drawing 10] It is drawing showing an example of the configuration of a group member managed table.
[Drawing 11] It is drawing showing an example of the information configuration set up as a security association.
[Drawing 12] It is drawing showing the procedure of group management processing.
[Drawing 13] It is drawing showing the procedure of group generation processing.
[Drawing 14] It is drawing showing the procedure of group participating processing.
[Drawing 15] It is drawing showing the procedure of the notice processing of a new member into a group.
[Drawing 16] It is drawing showing the procedure of group balking processing.
[Drawing 17] It is drawing showing the procedure of group control IP packet reception.
[Drawing 18] It is drawing showing the procedure of IP receive section at the time of IP packet reception.
[Drawing 19] It is drawing showing the procedure of the receiving access-control section at the time of IP packet reception.

[Drawing 20] It is drawing showing the network system constituted from a software configuration of a network device, and a network device.
[Drawing 21] It is drawing showing a hardware configuration and the storage information on a storage.
[Drawing 22] It is drawing showing the range of the first group communication link and the second group communication link.
[Drawing 23] It is drawing showing the connection phase of the network device which performs a group communication link.
[Drawing 24] It is drawing showing the procedure which performs user access control in the group management processing section.
[Drawing 25] It is drawing showing **** for the procedure of the right setting processing of user access.
[Drawing 26] It is drawing showing the frame structure exchanged between the network devices which perform other group communication links by processing of the right setting processing of user access.
[Drawing 27] It is drawing showing the example of 1 configuration of SA.
[Drawing 28] It is drawing showing the subgroup management procedure in the group management processing section.
[Drawing 29] It is drawing showing the procedure of subgroup access privilege check processing.
[Drawing 30] It is drawing showing the procedure of a user access condition process.
[Drawing 31] It is drawing showing the procedure of the IPsec transmitting processing section.
[Drawing 32] It is drawing showing an example of the system configuration which applies this invention.
[Drawing 33] It is drawing showing the procedure of subgroup access client processing.
[Drawing 34] It is drawing showing the frame structure exchanged with a host between nodes.
[Drawing 35] It is drawing showing the processing configuration of the group management processing section in the first node.
[Drawing 36] It is drawing showing the procedure in remote access control processing.
[Drawing 37] It is drawing showing the procedure in application proxy processing.
[Description of Notations]
100, 105, 106 -- A node, 107 -- A root group, 108 -- Subgroup, 207 -- A memory card, 301 -- Application, 302 -- Group management processing section, 308 -- An access polish database, 309 -- SA database, 314 -- IP receive section, 304 -- IP transmitting section, 312 -- IPsec reception section, 316 -- The receiving access-control section, 600 -- A group managed table, 700 -- The application managed table for an access control, 800 -- A group member managed table, 900 -- Security association, 2001 -- An access user managed table, 2002 -- An authentication key,

2100 -- User access control processing, 2150 -- Subgroup access privilege check processing, 2200 -- Subgroup management processing, 2400 -- Application proxy processing, 2500 -- Remote access control processing, 3100 -- A control section, 3200 -- The group generation processing section, 3300 -- Group participating processing section, 3400 [-- A host, 4301 / -- Subgroup access client processing.] -- The group balking processing section, 3500 -- The group information update process section, 3600 -- The group control IP packet reception section, 4201

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号
特開2004-254271
(P2004-254271A)

(43)公開日 平成16年9月9日(2004.9.9)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/08	H04L 9/00	601C	5J104
	H04L 9/00	601E	

審査請求 未請求 請求項の数 24 OL （全 46 頁）

(21)出願番号 特願2003-141286(P2003-141286)
(22)出願日 平成15年5月20日(2003.5.20)
(31)優先権主張番号 特願2002-375123(P2002-375123)
(32)優先日 平成14年12月25日(2002.12.25)
(33)優先権主張国 日本国(JP)

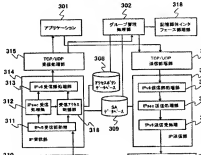
(71)出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人 100075096
弁理士 作田 康夫
(72)発明者 水谷 美加
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者 神牧 秀樹
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】ネットワーク機器、ネットワークシステム、および、グループ管理方法

(57)【要約】
【課題】利用者が認めた機器でグループを構成、グループに属する機器間の安全な通信を実現する。
【解決手段】グループ管理処理部３０２にて、グループ内の暗号通信に用いる暗号化鍵を作成し、暗号通信に必要な情報とともに自身の記憶部と記憶媒体とに格納する。その記憶媒体を用いて既にグループに属している他の機器に自身と暗号通信を行うために必要な情報を送信する。
グループから離脱する場合は、自身が補修している暗号通信を行うために情報を削除するとともに、他の機器に自身の離脱を通知し、通知を受けた機器内の離脱する機器に関する情報を削除してもらう。
前記グループ内の機器から、ユーザが選択した機器をサブグループとし、サブグループ内の暗号通信に用いる暗号化鍵を作成し、暗号通信に必要な情報及びサブグループ情報を、他のサブグループに属する機器に、前記グループの暗号化鍵を用いた暗号化通信により送信する。
【選択図】図３

図3



【特許請求の範囲】
【請求項１】
ネットワークを介して接続された他のネットワーク機器と通信を行なうネットワーク機器であって、
互いに認証可能な前記ネットワーク機器をグループとして管理するグループ管理手段と、
前記グループ所属するネットワーク機器間で共通の暗号化鍵による暗号通信を行う暗号通信手段と、
前記暗号化鍵の情報と前記グループに所属するネットワーク機器のホスト名およびアドレスを含む識別情報とを含む、前記グループに所属するネットワーク機器と暗号通信を行うために必要な暗号通信情報を格納する記憶手段と、
外部から情報を取得する取得手段と、を備え、
前記グループ管理手段は、
前記記憶手段に前記暗号通信情報が格納されていない状態で、前記取得手段において前記暗号通信情報を取得すると、当該暗号通信情報を前記記憶手段に格納するとともに、前記暗号通信手段を介して自身の識別情報を前記グループに所属するネットワーク機器に送信し、
前記暗号通信手段を介して他のネットワーク機器から当該他のネットワーク機器の識別情報を取得すると、前記記憶手段に記憶している前記暗号通信情報に当該識別情報を追加することを特徴とするネットワーク機器。
【請求項２】
請求項１記載のネットワーク機器であって、
前記グループ管理手段は、さらに、
前記取得手段においてグループから離脱する指示を受け付けると、前記記憶手段に記憶されている前記グループに所属する全てのネットワーク機器に、前記暗号通信手段を介して自身のネットワーク機器の離脱を通知するとともに、前記記憶手段から前記暗号通信情報を削除し、
前記暗号通信手段を介して他のネットワーク機器から、当該他のネットワーク機器が離脱する通知を受け付けると、前記記憶手段に記憶している前記暗号通信情報から、当該他のネットワーク機器の識別情報を削除する、
ことを特徴とするネットワーク機器。
【請求項３】
請求項１または２のいずれかに記載のネットワーク機器であって、
前記取得手段は、記憶媒体のインタフェースであり、
前記グループ管理手段は、さらに、
前記記憶手段に前記暗号通信情報が格納されている状態で、前記暗号通信情報が格納された記憶媒体が前記取得手段に挿入された場合、前記記憶手段に格納されている暗号通信情報を前記記憶媒体にコピーすることを特徴とするネットワーク機器。
【請求項４】
請求項１、２、または、３のいずれかに記載のネットワーク機器であって、
非暗号通信を行なう非暗号通信手段と、
前記ネットワーク機器が提供するサービスに対するアクセスを制御するアクセス制御手段とをさらに備え、
前記アクセス制御手段は、前記非暗号通信手段を介して他のネットワーク機器からアクセスがあった場合、前記アクセスが予め定められたポートに対するものである場合、前記アクセスを許可することを特徴とするネットワーク機器。
【請求項５】
複数のネットワーク機器と、前記複数のネットワーク機器を接続するネットワークとを備えたネットワークシステムにおいて、
前記複数のネットワーク機器は、請求項１乃至４のいずれかに記載のネットワーク機器である

ことを特徴とするネットワークシステム。
【請求項６】
ネットワークを介して接続された他の機器と、互いに認証可能な暗号通信を行なうグループを管理するグループ管理方法であって、
前記ネットワークに接続された一つの機器において、前記暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と自機器のホスト名とアドレスとを含む識別情報とを暗号通信情報として保有するグループ生成ステップと、
前記暗号通信情報を取得した機器において、前記暗号通信情報に前記識別情報が格納されている全機器に自身の識別情報と参加を示す情報とを前記暗号通信により通知し、当該暗号通信情報に自身の識別情報を追加して保有する第１のグループ参加ステップと、
当該識別情報と前記参加を示す情報とを受けた機器において、自身が保有する前記暗号通信情報に当該識別情報を追加する第２のグループ参加ステップと、
前記グループから離脱する指示を受け付けた機器において、自身を除く前記暗号通信情報に前記識別情報が格納されている全機器に離脱を示す情報と自身の識別情報とを前記暗号通信により通知し、自身の保有する前記暗号通信情報を削除する第１のグループ離脱ステップと、
当該離脱の通知を受けた機器において、自身が保有する前記暗号通信情報から通知を受けた識別情報を削除する第２のグループ離脱ステップとを備えることを特徴とするグループ管理方法。
【請求項７】
コンピュータを、
暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と自身のホスト名およびアドレスを含む識別情報とを暗号通信情報として保有するグループ生成手段と、
前記暗号通信情報を取得すると、前記暗号通信情報に前記識別情報が格納されている全機器に自身の識別情報と参加を示す情報とを前記暗号通信により通知し、前記暗号通信情報に前記自身の識別情報を追加して保有する第１のグループ参加手段と、
他の機器から当該機器の識別情報と参加を示す情報とを受信すると、自身が保有する前記暗号通信情報に当該識別情報を追加する第２のグループ参加手段と、
前記暗号通信情報を削除する指示を受け付けると、自身を除く前記暗号通信情報に前記識別情報が格納されている全機器に離脱を示す情報と前記自身の識別情報とを前記暗号通信により通知し、自身の保有する前記暗号通信情報を削除する第１のグループ離脱手段と、
他の機器の識別情報と前記離脱を示す情報とを受信すると、自身が保有する前記暗号通信情報から受信した識別情報を削除する第２のグループ離脱手段、
として機能させるためのプログラム。
【請求項８】
請求項１または２記載のネットワーク機器であって、
前記ネットワークに接続された第１のグループに含まれるネットワーク機器を表示し、選択可能なインタフェース手段を有し、
前記グループ管理手段は、前記選択されたネットワーク機器を第２のグループとして管理し、
前記記憶手段は、前記第２の暗号化鍵と前記第２のグループに所属するネットワーク機器のホスト名とアドレスを含む識別情報を含む暗号通信情報を格納し、
前記暗号通信手段は、前記第２のグループで共通の第２の暗号化鍵による暗号通信を行うことを特徴とするネットワーク機器。
【請求項９】
請求項８記載のネットワーク機器であって、
前記第１のグループの暗号化鍵を用いて暗号化された前記暗号通信情報を前記第２のグループに所属するネットワーク機器に対して送信する手段を有することを特徴とするネットワーク機器。
【請求項１０】

請求項８記載のネットワーク機器であって、
前記記憶手段は、前記第１のグループの暗号化鍵で暗号化された前記暗号通信情報を他のネットワーク機器から取得した場合、前記第２のグループの暗号通信情報として格納し、前記第２の暗号鍵を用いた暗号通信による第２のグループ通信を行うことを特徴とするネットワーク機器。
【請求項１１】
請求項８記載のネットワーク機器であって、
ユーザが第２のグループに対応するユーザ識別情報と秘密情報を設定できる前記インタフェース手段と、
前記ユーザ識別情報、秘密情報、前記第２のグループの暗号通信情報と対応した第２のグループ識別子、自ネットワーク機器において生成した認証鍵とからなるグループ情報を格納する前記記憶手段と、
前記第２のグループ情報を記憶媒体に格納する手段と、
前記第２のグループ情報を前記第１のグループの暗号化鍵で暗号化し、第２のグループに属する全てのネットワーク機器に対して送信する手段とを有し
前記記憶手段は、暗号化された前記第２のグループ情報を受信すると、前記第１の暗号化鍵を用いて復号化された前記グループ情報を格納することを特徴とするネットワーク機器。
【請求項１２】
請求項１１記載のネットワーク機器であって、
自機器が管理しているユーザ識別情報と秘密情報を前記記憶媒体に記憶された値と同一であることを確認する手段と、
前記記憶媒体に記憶されているグループ識別情報に対応する機器が管理する第２の暗号鍵を検索する手段を備え、
前記第２の暗号鍵を用いて前記第２のグループ間で暗号通信を行うことを特徴とするネットワーク機器。
【請求項１３】
請求項８または１１のいずれか記載のネットワーク機器であって、
前記インタフェース手段を有しているネットワーク機器は、暗号化された前記第２のグループ情報を受信した場合、前記第１の暗号化鍵を用いて復号化し、前記グループ情報を前記記憶手段に格納することを特徴とするネットワーク機器。
【請求項１４】
請求項８または１１のいずれか記載のネットワーク機器であって、
前記第２のグループに属する他のネットワーク機器との通信を必要とするアプリケーションを起動する場合、前記アプリケーションの送信元ポート番号を格納する記憶手段と、
前記アプリケーションからパケットが送信される場合、前記パケットの送信元ポート番号と記憶している前記管理ポート番号が一致を確認する手段と、を備え、
一致している場合のみの前記第２の暗号鍵を用いた暗号通信による第２のグループ通信により前記パケットの送信すること特徴とするネットワーク機器。
【請求項１５】
請求項８または１１のいずれか記載のネットワーク機器において、
前記記憶媒体に前記グループ情報を格納しているネットワーク機器のアドレスを、前記記憶媒体に追加して格納する記憶手段を備えることを特徴とするネットワーク機器。
【請求項１６】
請求項８または１１のいずれか記載のネットワーク機器において、
前記記憶媒体に前記グループ情報を格納すると共に、
前記第２のグループに属する全てのネットワーク機器の名前とアドレスを前記記憶媒体に追加格納することを特徴とするネットワーク機器。
【請求項１７】
複数のネットワーク機器と、前記複数のネットワーク接続機器を接続するネットワークと

を備えたネットワークシステムにおいて、前記複数のネットワーク機器は、請求項８から請求項１６のいずれかのネットワーク機器であることを特徴とするネットワークシステム。

【請求項１８】
グループ通信を行う第１のネットワーク機器とグループ通信を行わない第２のネットワーク機器が接続されるネットワークシステムにおいて、
前記第２のネットワーク機器は、
請求項１５記載の記憶媒体を介して、記憶媒体上のユーザ識別子、秘密情報、グループ識別子、認証鍵及びアドレスを読み出す手段と、
ユーザがユーザ識別子と秘密情報を入力するインタフェース手段と、
記憶媒体上のユーザ識別子と秘密情報とを入力した値が一致していることを確認する手段と、
前記ユーザ識別子と秘密情報を認証鍵で暗号化し、前記暗号化したユーザ識別子と秘密情報、グループ識別子を前記アドレス宛に送信する手段と、
前記認証鍵で暗号化された第２の共通の暗号化鍵を受信する手段を備え、
前記ユーザが通信を行う場合、前記第２の共通の暗号化鍵による暗号通信を行うことを特徴とするネットワーク機器。

【請求項１９】
請求項１８記載の第２のネットワーク機器において、
請求項１６記載の記憶媒体を介して、記憶媒体上のネットワーク機器の名前とアドレスをユーザに表示する手段と、
ユーザが表示されたネットワーク機器から接続したいネットワーク機器を選択する手段と、
ユーザが選択したネットワーク機器のアドレスに対し、記憶媒体上の認証鍵で暗号化したユーザ識別子と秘密情報、グループ識別子を送信する手段とを備えることを特徴とするネットワーク機器。

【請求項２０】
請求項１８または１９のいずれか記載のネットワーク機器であって、
前記第１のネットワーク機器は、
前記第２のネットワーク機器において前記暗号化したユーザ識別子と秘密情報、グループ識別子を受信する手段と、
前記受信したグループ識別子より、機器で管理するグループ識別子と対になる認証鍵を検索する手段と、
前記認証鍵を用いてユーザ識別子と秘密情報を復号化する手段と、
グループ識別子と対応する機器で管理するユーザ識別子と秘密情報が一致するか否かを確認する手段と、
前記グループ識別子と対になる機器で管理する第２の共通の暗号化鍵を前記認証鍵で暗号化し、第２のネットワーク機器へ送信する手段と、を備え、
第２のネットワーク機器との通信に対し、第２の共通の暗号化鍵にて暗号化通信を行うことを特徴とするネットワーク機器。

【請求項２１】
ネットワークシステムであって、
グループ通信を行う請求項２０記載のネットワーク機器とグループ通信を行わない請求項１８または１９のいずれか記載のネットワーク機器が接続されることを特徴とするネットワークシステム。

【請求項２２】
請求項６記載のグループ管理方法であって、
グループに属するネットワーク機器が選択される選択ステップと、
前記選択されたネットワーク機器間で、互いに認証可能な暗号通信に用いる他の暗号化鍵を生成し、当該他の暗号化鍵と前記第２のグループに属するネットワーク機器のホスト名

とアドレスを含む識別情報を含む暗号通信情報を保有する第２のグループ暗号情報生成ステップと、
前記暗号通信情報を、前記暗号化鍵を用いて暗号化して前記第２のグループに属するネットワーク機器に対して通知する第２のグループ暗号情報配布ステップと、
前記第２の暗号通信情報を受けた機器が当該第２の暗号通信情報を保有するグループ参加ステップと、
ユーザ識別情報、ユーザが作成した秘密情報、前記第２のグループの暗号通信情報と対応した第２のグループ識別子、及び生成した認証鍵とからなるグループ情報を保有し、記憶媒体に前記情報を格納する第２のグループ情報生成ステップと、
前記暗号化鍵を用いて、第２のグループのグループ情報を暗号化し、前記第２のグループに属するネットワーク機器に対して通知する第２のグループ情報配布ステップと、
前記第２のグループ情報を受けた機器が前記グループ情報を保有するグループアクセス権設定ステップとを有することを特徴とするグループ管理方法。
【請求項２３】
請求項２２記載のグループ管理方法であって、
機器が管理しているユーザ識別情報と秘密情報が、前記記憶媒体上の値と同一であることを確認するユーザ認証ステップと、
アプリケーションのポート番号を保有する暗号通信準備ステップとを備えることを特徴とするグループ管理方法。
【請求項２４】
請求項７記載のプログラムにおいて、
グループに属するネットワーク機器が選択される選択手段と、
前記選択したネットワーク機器間で、互いに認証可能な暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と前記第２のグループに所属するネットワーク機器のホスト名とアドレスを含む識別情報を含む暗号通信情報を記憶する第２のグループ暗号情報生成手段と、
前記暗号化鍵を用いて、第２のグループの暗号通信情報を暗号化し、前記第２のグループに所属するネットワーク機器に対して通知する、第２のグループ暗号情報配布手段と、
前記第２の暗号通信情報を受けた機器において、暗号通信情報を保有するグループ参加手段と、
ユーザ識別情報、ユーザが作成した秘密情報、前記第２のグループの暗号通信情報と対応した第２のグループ識別子、及び生成した認証鍵とからなるグループ情報を記憶し、記憶媒体に前記情報を格納する第２のグループ情報生成手段と、前記暗号化鍵を用いて、第２のグループのグループ情報を暗号化し、前記第２のグループに所属するネットワーク機器に対して通知する、第２のグループ情報配布手段と、
前記第２のグループ情報を受けた機器において、グループ情報を記憶するグループアクセス権設定手段と、
ユーザがネットワーク機器を利用する場合、前記記憶媒体を介して、機器が管理しているユーザ識別情報と秘密情報を前記記憶媒体上の値と同一であることを確認するユーザ認証手段と、
ユーザが利用するアプリケーションのポート番号を保有する暗号通信準備手段と、
第２のグループに属する機器へパケット送信する場合、送信パケットのポート番号が保有していると一致する場合、第２のグループの暗号化鍵による暗号通信を行う手段、
として機能させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワークに接続する特定の機器間で排他的かつ安全に通信を行う技術に関する。
【０００２】
【従来の技術】

Ｉｎｔｅｒｎｅｔ　ＰｒｏｔｏｃｏＩ（以下、ＩＰと呼ぶ）と呼ばれる通信プロトコルを使用するＩＰネットワークは、コンピュータネットワークのデファクトスタンダードとしての地位を確立し、一般ユーザへの普及が著しい。

【０００３】

このＩＰネットワークを介して機器間でデータをやりとりするには、その機器それぞれに一意的にＩＰアドレスを付与することが必要である。現在では、ＩＰアドレスを３２ビットで表すＩＰｖ４（Ｉｎｔｅｒｎｅｔ　ＰｒｏｔｏｃｏＩ　ｖｅｒｓｉｏｎ　４）が用いられているが、ＩＰネットワークの利用が増大するに連れて、ＩＰアドレスの不足が大きな問題となってきている。

【０００４】

このような状況を背景に、ＩＰアドレスを１２８ビットに拡張し、さらに、セキュリティ機能など、今までのＩＰアドレスになかった機能を付加した新しいＩＰアドレスを用いるＩＰネットワークとしてＩＰｖ６（Ｉｎｔｅｒｎｅｔ　ＰｒｏｔｏｃｏＩ　ｖｅｒｓｉｏｎ　６）がＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）にて採択され、それを用いたネットワークサービスが次世代ＩＰとして標準化されつつある。

【０００５】

さらに、使用可能なアドレス数が増え、セキュリティ機能が充実したＩＰｖ６の新たな適用先として、冷蔵庫、洗濯機などの白物家電、あるいはテレビ、ビデオといったＡＶ機器といった家庭内の機器から構成されるホームネットワークなどが注目されている。

【０００６】

これらの機器それぞれにＩＰアドレス割り当てることにより、各機器をサーバとみなすことができるようになり、機器間通信により新しいサービスを実現したり、外部端末からの機器の制御、サービスセンタからの機器の制御といったインターネットを介した新しいサービスを実現するといったことが考えられている。

【０００７】

ところで、家庭内機器のような特定の機器間の通信においては、利用者が認識している範囲外の機器からの操作を排除するようなシステムが要求される。例えば、友人が持ってきた機器による勝手な操作の防止が必要である。

【０００８】

すなわち、利用者が互いの通信を許可する範囲を決定し、それらの機器をグループ化し、グループ化された機器間でのみ通信がなされるようなシステムが要求される。そして、このような通信を実現するためには、グループ内の機器間で、互いをグループ内に属する真正な機器であることを認証するための認証機能が必要である。

【０００９】

このような認証機能として、従来のクライアント、サーバ型のシステムでは、認証サーバを用いたものが実現されている。例えば、ＲＦＣ２８６５で定義されるＲＡＤＩＵＳ（Ｒｅｍｏｔｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ＤｉａｌｉｎＵｓｅｒ　Ｓｅｒｖｉｃｅ）では、サーバにアクセスするクライアントのアカウント（ユーザ名、パスワード）をＲＡＤＩＵＳサーバと呼ばれる認証サーバで一括管理し、サーバは、クライアントからのアクセス要求（ユーザ名、パスワードを含む）をＲＡＤＩＵＳサーバに転送しアクセス可否の判断結果を受けて、クライアントとの通信を行うかどうか判断する。

【００１０】

例えば、従来のグループ化された特定の機器間での暗号通信システム及びその通信方法としては、例えば、特許文献１あるいは特許文献２に示されているものがある。

【００１１】

【特許文献１】特開２００２－１２４９４１号公報

【特許文献２】特開平５－３４７６１６号公報

【００１２】

【発明が解決しようとする課題】

ホームネットワークに接続されている機器の中で、利用者が指定した機器間でのみ所定の通信を行うためには、互いに相手が指定された機器であることを認証する機能が必要と考えられている。

【００１３】

従来の認証機能は、クライアント・サーバシステムが前提であり、サーバにアクセスするクライアントのアクセス情報を管理する認証サーバを備えることで実現されている。

【００１４】

これに対し、ホームネットワークを構成する機器は、適宜サービスに応じて必要な機器間で通信を行なうといったアドホック型である。このため、全ての機器がサーバにもクライアントにもなり得、アクセス情報の設定がより煩雑になるという問題がある。

【００１５】

このような場合に、従来のように認証サーバを備え、機器間でのセッション確立毎、あるいはサービス開始毎に個別に認証を行うようにすると、認証のオーバヘッドが大きくなるという問題もある。

【００１６】

例えば、前述の特許文献１に開示された技術は、認証機能を有したグループ通信システムである。本技術は、グループを構成する機器以外に、グループ通信システム内にグループ暗号鍵を生成する機能及びグループに所属する端末情報を管理する機能を備えたグループ暗号鍵管理部と及び中継装置とを備えて構成され、大規模なネットワーク構成を前提としたものである。

【００１７】

また、前述の特許文献２に開示された技術は、まず、グループ通信を行う機器ごとにＩＣカードを具備していなければならない。そして、そのＩＣカードには、予め送受信相手の所属ごとに設定された複数のマスタ鍵とグループ鍵生成プログラムとが記録されている必要がある。

【００１８】

このように、従来の技術では、実際に通信を行なう機器以外に認証サーバとなる機器を用意する必要があったり、マスタ鍵と個々の通信相手先の関係といった複雑な情報を予め記憶させておく記録媒体をグループを構成する機器の数だけ用意する必要があった。

【００１９】

機器のグループを構成し、その機器間で認証を行い、安全な通信を実現したとしても、第三者による機器の利用を妨げることが出来ない為、ユーザが予期しない勝手な操作が行われる可能性がある。すなわち、グループを利用するユーザ及び機器を利用するユーザレベルのアクセス制御ができないという問題がある。

また、ユーザにより利用できる機器を制限することもできないという問題がある。

加えて、家庭内ネットワークといった、場所が固定されたローカルネットワークに配置された機器間の通信にしか適用できない。これは、ＩＰｓｅｃを利用していることから、グループを構成する機器であるかを判断する為に共有鍵に加えて送信先ＩＰアドレス及び受信元ＩＰアドレスのペアが固定である必要がある事に因る。グループを構成していた機器がローカルネットワークから移動した場合、グループ通信によるアクセス制御が適用できないという課題がある。

【００２０】

本発明は、このような事情に鑑みなされたもので、本発明の目的は、利用者が認めた機器間で容易に互いを認証し合うことが可能なグループを構成し、そのグループに属する機器間の安全な通信を実現することにある。

【００２１】

さらに、本発明の他の目的は、グループ内の機器が提供するアプリケーションにグループ外の機器にもアクセスを許可するものがある場合、グループ外の機器から、そのアプリケーションにのみアクセスを許可するといったアクセス制御を実現することにある。

【００２２】

本発明の他の目的は、ユーザが認めた機器間で構成したグループ内において、ユーザを限定するサブグループを構成すると共に、サブグループを利用するユーザのアクセス制御を実現することである。

【００２３】

本発明の他の目的は、ユーザが物理的な距離が離れたところから、サブグループを構成する機器への安全なアクセス／制御を実現することにある。

【００２４】

尚、本願は上記目的のうちの少なくともひとつを解決するものである。

【００２５】

【課題を解決するための手段】

本発明は、共有の鍵を用いて暗号通信を行うことで互いを認証し、セキュリティの確保された通信を行なう機器の集まりをグループとみなし、そのグループを構成する機器となりうる個々の機器のいずれもが、グループを生成し、参加し、また、そのグループから離脱するといったグループ管理の手段を有する。

【００２６】

また、機器がいずれかのグループに属していても、グループ外の機器との通信の可能性も保有するものである。

【００２７】

具体的には、ネットワークを介して接続された他のネットワーク機器と通信を行なうネットワーク機器であって、互いに認証可能な前記ネットワーク機器をグループとして管理するグループ管理手段と、前記グループ所属するネットワーク機器間で共通の暗号化鍵による暗号通信を行う暗号通信手段と、前記グループに所属するネットワーク機器の、ホスト名とアドレスとを含む識別情報および前記暗号化鍵の情報を含む前記グループに所属するネットワーク機器と暗号通信を行うために必要な暗号通信情報を格納する記憶手段と、外部から情報を取得する取得手段と、を備え、前記グループ管理手段は、前記記憶手段に前記暗号通信情報が格納されていない状態で、前記取得手段において前記暗号通信情報を取得すると、当該暗号通信情報を前記記憶手段に格納するとともに、前記暗号通信手段を介して自身の識別情報を前記グループに所属するネットワーク機器に送信し、前記暗号通信手段を介して他のネットワーク機器から当該他のネットワーク機器の識別情報を取得すると、前記記憶手段に記憶している前記暗号通信情報に当該識別情報を追加することを特徴とするネットワーク機器を提供する。

【００２８】

また、前記グループ管理手段は、さらに、前記取得手段においてグループから離脱する指示を受け付けると、前記記憶手段に記憶されている前記グループに所属する全てのネットワーク機器に、前記暗号通信手段を介して自身のネットワーク機器の離脱を通知するとともに、前記記憶手段から前記暗号通信情報を削除し、前記暗号通信手段を介して他のネットワーク機器から、当該他のネットワーク機器が離脱する通知を受け付けると、前記記憶手段に記憶している前記暗号通信情報から、当該他のネットワーク機器の識別情報を削除する、ことを特徴とするネットワーク機器を提供する。

前記第一のグループを構成するネットワーク機器において、ユーザが利用できるネットワーク機器を選択し、それら機器に対して前記暗号通信手段を介して、選択したネットワーク機器で利用する第二の暗号鍵を配布することにより、第一のグループ内に第二のグループを構成し、第二の共通の暗号鍵を用い暗号通信を行うことで、互いを認証し、セキュリティの確保された通信を行うものである。

また、第二の暗号鍵と対応したユーザの識別子とパスワードの情報をネットワーク機器と記憶媒体で管理すると共に、第一の暗号鍵で前記情報を暗号化して他の第二のグループ通信を行うネットワーク機器へ配布することにより、ユーザがネットワーク機器を利用する際、どのネットワーク機器においても、記憶媒体の情報とネットワーク機器の情報が一致することを確認することにより、グループ通信の利用可否のアクセス制御を提供する。

記憶媒体でネットワーク機器のアドレスと認証鍵を管理し、ネットワーク機器において認

証鍵を管理し、第一の暗号鍵で暗号化して他の第二のグループ通信を行うネットワーク機器へ管理を依頼することにより、グループ通信対象でないネットワーク機器からユーザが第二のグループ通信対象のネットワーク機器と通信を開始する際、記憶媒体の認証鍵で、記憶媒体のパスワードとユーザＩＤを暗号化し、その暗号化情報を記憶媒体のアドレス宛てに送信し、第二のグループ通信対象のネットワーク機器では認証鍵でユーザＩＤとパスワードを復号化し、ユーザＩＤとパスワードを確認した上で、第二の共通の暗号鍵を認証鍵で暗号化して、返送することにより、グループ通信対象でないネットワーク機器との間で第二の暗号鍵での暗号通信を提供する

【００２９】

【発明の実施の形態】

以下、本発明の実施の形態を、図を用いて説明する。

【００３０】

本実施形態では、宅内において家電などにより構成されるネットワークに本発明を適用した場合を例にあげ、説明する。

【００３１】

本実施形態の宅内のネットワークは、ＩＰｖ６により構成され、それぞれにＩＰアドレスが付与された、例えば、電子レンジやエアコンなどの家電機器、テレビやビデオなどのＡＶ機器、センサ等が接続されている。以下、ネットワークに接続され、ＩＰｖ６によるＩＰアドレスを付与されている各機器を、ノードと呼ぶこととする。

【００３２】

本実施形態では、これらのノードのうち、利用者が互いに通信を行なうことを許可したものをグループとし、グループに属するノード間で認証のために共通の暗号化鍵による暗号通信を行なう。

ここで、本ネットワークで採用しているＩＰｖ６は、前述したように、確保できるＩＰアドレス数が莫大となるだけでなく、ＩＰｓｅｃと呼ばれる暗号・認証の仕組みが標準で装備され、高度な安全性を保ちながら、使い勝手もよいという特徴を持つ。本実施形態においては、ＩＰｖ６のＩＰｓｅｃを用いて、グループを構成する機器間のみでの安全な通信を実現する。

本実施形態の詳細な説明の前に、まず、ＩＰｓｅｃの概要について説明する。

ＩＰｓｅｃは、ＩＰ層において相互接続可能で高品質な暗号化ベースのセキュリティを提供する技術である。このセキュリティは、認証ヘッダＡＨ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ）とＩＰ暗号化ペイロードＥＳＰ（ＥｎｃａｐｓｕＩａｔｉｏｎ Ｓｅｃｕｒｉｔｙ ＰａｙＩｏａｄ）の２つのトラフィックセキュリティプロトコル等によって実現されている。

【００３３】

ＡＨは、ＩＰパケットの改ざんを防ぐ機能を提供し、ＥＳＰは、ＩＰパケットを暗号化し、かつ、その認証データを格納することで、ＩＰパケットの機密性と完全性とを保証するものである。

【００３４】

ＡＨ、ＥＳＰ共に、認証鍵、暗号鍵を用いて、それぞれ認証情報、暗号データを作成し、送付した暗号化されたデータを解読可能な鍵を保有しているか否かにより通信相手の機器を認証する。

【００３５】

図４と図５とに、それぞれ、ＡＨプロトコルおよびＥＳＰプロトコルを利用した場合のＩＰパケットの構成を示す。なお、これらのパケット構成は、ＩＰｓｅｃパケットとしてＲＦＣ２４０１～２４０３に規定されているものである。

【００３６】

図４は、ＡＨプロトコルを利用した場合のＩＰパケットの構成を示すものである。この場合のＩＰパケットは、ＩＰヘッダ４００と、ＴＣＰ／ＵＤＰヘッダ４０２と、データ４０３に対するハッシュ値を格納するＡＨヘッダ４０１とを備える。

【００３７】
ＡＨヘッダ４０１に格納されているハッシュ値は、パケットが改ざんされていないことを証明するためのもので、通信相手間で相互に保有する認証鍵を用いて計算された値が格納される。これは、認証されているもの同士では同じ認証鍵を保有することが前提となっているもので、送信側で自身が保有する認証鍵によって計算して格納したデータのハッシュ値を、受信側が、自身が保有する認証鍵によって計算したデータのハッシュ値と比較し、両者が合致することにより、相手が同じ認証鍵を保有するものであることを確認することができる。すなわち、パケットの送信相手が同じ暗号化鍵を保有するグループ内の機器であることが証明される。
【００３８】
図５はＥＳＰプロトコルを利用した場合のＩＰパケットの構成を示すものである。ＴＣＰ／ＵＤＰヘッダと、データを暗号化した場合のヘッダ構成である。
【００３９】
この場合のＩＰパケットは、暗号化しているパケットであることを示すＥＳＰヘッダ５０１と、暗号化の区切りを揃えるためのＥＳＰトレーラ５０４と、認証データ５０５とを備える。認証データ５０５はオプションであり、ＥＳＰヘッダ５０５と、暗号化されたＴＣＰ／ＵＤＰヘッダ５０２と、データ５０３と、ＥＳＰトレーラ５０４とのハッシュ値を格納するものである。
【００４０】
認証データ５０５に格納されるハッシュ値は、ＩＰペイロードの完全性を確保し、暗号化して転送するＴＣＰ／ＵＤＰヘッダ５０２およびデータ５０３の機密性を確保する。暗号化を行なう際には送信側が保有する暗号鍵を用いる。送信側が自身が保有する暗号鍵を用いて暗号化したデータを受信側は自身が保有する暗号鍵で復号する。受信側において、復号ができれば、相手が同じ暗号鍵を保有することが確認できる。すなわち、パケット送信相手が同じ暗号鍵を保有するグループ内機器であることの証明となる。
【００４１】
また、ＩＰｓｅｃで使用する暗号／認証アルゴリズム、鍵など、各機器間でＩＰｓｅｃの規格に従って通信を行う（以後、ＩＰｓｅｃの規格に従って行う通信のことをＩＰｓｅｃ通信と呼ぶ）ために共有すべき情報は、セキュリティアソシエーション（ＳＡ）として管理される。
【００４２】
ＳＡは、それによって運ばれるトラフィックに対してセキュリティサービスを提供する単方向の「コネクション」である。このため、ＩＰｓｅｃ通信を行うにあたって、通信を行う機器間で一方向の通信ごとに、予め設定を行う必要がある。すなわち、両方向の通信を行なうためには、送信方向と受信方向とのそれぞれのＳＡを設定する必要がある。
【００４３】
なお、ＩＰｓｅｃの詳細は、ＲＦＣ２４０１”Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ”に規定されている。
【００４４】
図１は、本発明を適用した一実施形態に係るグループ通信システムの構成を示す図である。
【００４５】
本図に示すように、本実施形態においては、４つのノード１００（１００Ａ、１００Ｂ、１００Ｃ、１００Ｄ）がＩＰｖ６によるネットワーク１１０に接続されている。もちろん構成ノード数はこれに限られない。
【００４６】
これらのノード１００間で、ネットワーク１１０を介してＩＰパケット形式のコマンドを送受信することにより、ノード１００各々が備える機器特有のサービス機能に対する他のノード１００からの操作、および、他のノード１００へのサービス提供が実現される。
【００４７】

具体的には、ネットワークを介して、テレビからエアコンの温度調節をしたり、テレビからの操作により、ビデオカメラで撮影している画像をビデオに送信し、ビデオカメラで撮影した画像をビデオで録画させるといったことが実現されるものである。

【００４８】

例えば、ノード１００Ａ～ノード１００Ｃは、利用者が相互にサービスを利用することを許可しているグループに属するノードであり、ノード１００Ｄは、そのグループ外のノードとすると、グループを構成するノード１００Ａ、１００Ｂ、１００Ｃ間では、サービス機能の利用要求を送信する際に、要求元ノードは、グループで共有する鍵（以後、グループ鍵と呼ぶ）により計算されたハッシュ値を格納した、または、暗号化したＩＰパケットを送付する（１０１方向）。利用要求を受け取った要求先ノードは、自身の保有するグループ鍵により要求元ノードがグループ構成ノードであることを確認し、サービス機能を要求元ノードに提供する（１０２方向）、といったＩＰｓｅｃ通信を行なう。

【００４９】

これに対し、ノード１００Ｄからは、サービス機能の利用要求は、通常のＩＰパケットによって送信することとなるため、ノード１００Ｃに通常のＩＰパケットを送信すると（１０４方向）、ノード１００Ｃにおいてグループ外ノードと判断され、サービス提供拒否のパケットの返答を受けることとなる（１０３方向）。

【００５０】

ここで、ノード１００Ｂがグループ外のノード１００に提供を許可するサービスを有するノードの場合、ノード１００Ｄからそのサービスの提供を指定して通常のＩＰパケットを送信すると（１０４ｂ方向）、ノード１００Ｂよりそのサービスが提供される（１０３ｂ方向）。

【００５１】

本実施形態では、以上のようにＩＰｓｅｃの仕組みを標準で実装するＩＰｖ６を用いたプロトコルによる通信が可能なネットワークを例にあげて説明する。しかし、グループを構成するノード１００間に共通の暗号化鍵を持たせ、その鍵を認証鍵または暗号鍵として当該グループ間で通信を行うことができる環境を構築できるならば、通信プロトコルはこれに限られない。

【００５２】

以下、このようなネットワークに接続されたノード１００間で、所定のサービスの安全な利用を実現するグループの管理方法、すなわち、一つのノード１００においてグループを生成し、生成されたグループに他のノード１００が参加し、また、生成されたグループから離脱する方法について説明する。

【００５３】

本実施形態では、空のメモリカードＡ、Ｂの２つを用意し、最初にグループに参加するノード１００において、グループ内でＩＰｓｅｃ通信を行うために必要な情報を生成し、そのうちの一つのメモリカードＡに、登録する。その後参加するノード１００は、メモリカードＡから必要な情報を取得することで、グループに参加する。また、グループから離脱する際は、空のメモリカードＢを用いる。

【００５４】

図２にノード１００のハードウェア構成を、図３にその機能構成を示す。

【００５５】

ノード１００は、ノード１００が備える一つ以上の固有機能部２０２と、ネットワークカード２０５と、固有機能部２０２及びネットワークカード２０５を制御するプロセッサ２００と、プロセッサ２００で実行するプログラムを記憶するメモリ２０１と、プログラム及び設定情報を記憶するハードディスク等の外部記憶装置２０４と、グループ情報を受け渡すためのメモリカード等のインタフェースを提供する記憶媒体インタフェース２０６と、これらを接続するシステムバス２０３とを備える。

【００５６】

なお、固有機能部２０２が実現する固有機能とは、例えばエアコンであれば、例えば冷暖

房機能、温度管理機能、タイマ機能等を司る処理部などのことである。

【００５７】

また、記憶媒体インタフェース２０６は、挿入する記憶媒体に書き込み中であることを利用者に通知するＬＥＤ（発光ダイオード）ライトを具備している。

【００５８】

次に、各ノード１００が備える機能を図３に従って説明する。これらの機能により、ノード１００は、ネットワークを介して、利用者がサービスの相互利用を許可したグループを構成するノード１００間でサービスの提供を実現する。

【００５９】

各ノード１００は、アプリケーション３０１と、グループ管理処理部３０２と、ＴＣＰ／ＵＤＰ送信処理部３０３と、ＩＰ送信部３０４と、アクセスポリシデータベース３０８と、ＳＡデータベース３０９と、ネットワークインタフェース受信処理部３１０と、ＩＰ受信部３１４と、ＴＣＰ／ＵＤＰ受信処理部３１５と、ネットワークインタフェース送信処理部３１７と、記憶媒体インタフェース処理部３１８とを備える。

【００６０】

アプリケーション３０１は、各ノード特有のサービスを提供するものである。

【００６１】

グループ管理処理部３０２は、後述するグループの生成、離脱、更新など、グループに関する管理を行なうものである。

【００６２】

ネットワークインタフェース受信処理部３１０とネットワークインタフェース送信処理部３１７とは、ネットワークカードを制御するものである。

【００６３】

記憶媒体インタフェース処理部３１８は、記憶媒体インタフェース２０６を制御するものである。記憶媒体インタフェース３１８は、メモリカード等の記録媒体が記録媒体インタフェース２０６に挿入されたことを検出すると、記憶媒体インタフェース２０６に備えられているＬＥＤライトを点灯し、メモリカードを利用中であることを利用者に対して示す。また、グループ管理処理部３０２から処理終了の通知を受けると、記憶媒体インタフェース２０６に備えられているＬＥＤライトを消灯し、利用者に対し、メモリカード等の記憶媒体への書込みが終了したこと、および、グループ管理処理部３０２における処理が完了したことを通知する。

【００６４】

なお、通知を受けた利用者は、メモリカードを当該記憶媒体インタフェース２０６から取り出すことができる。

【００６５】

ＴＣＰ／ＵＤＰ送信処理部３０３と、ＩＰ送信部３０４と、ＩＰ受信部３１４と、ＴＣＰ／ＵＤＰ受信処理部３１５とは、送受するＩＰパケットに対し、各層の処理を行い、通信を実現するものである。

【００６６】

ＩＰ送信部３０４は、ＩＰｖ６送信前処理部３０５と、ＩＰｓｅｃ送信処理部３０６と、ＩＰｖ６後処理部３０７とを備え、ＩＰ受信部３１４は、ＩＰｖ６受信前処理部３１１と、ＩＰｓｅｃ受信処理部３１２と、ＩＰｖ６受信後処理部３１３とを備える。ＩＰ送信部３０４とＩＰ受信部３１４とで、ＩＰｖ６による通信を実現する。

【００６７】

ここで、ＩＰｖ６受信前処理部３１１は、ＩＰヘッダを構成するバージョン、ペイロード長、ホップ・リミットの設定値の確認およびオプションヘッダ（ＡＨとＥＳＰとを除く）処理といったＩＰｖ６受信前処理を行なうものである。ＩＰｖ６受信前処理部３１１は、受け取ったＩＰパケットにＡＨヘッダまたはＥＳＰヘッダのいずれかが付加されていた場合、そのＩＰパケットをＩＰｓｅｃ処理部３１２に受け渡す。いずれのヘッダも付加されていなかった場合、そのＩＰパケットを後述する受信アクセス制御部３１６に受け渡す。

【００６８】
ＩＰｓｅｃ処理部３１２は、ＩＰヘッダのオプションヘッダのうち、ＡＨとＥＳＰの処理を行ない、受信したＩＰパケットがグループに属するノード１００から送信されたものか否かを判断する。
【００６９】
ＩＰｖ６受信後処理部３１３は、ＩＰパケットを受け取ると、送信元ＩＰアドレス、送信先ＩＰアドレスを含むＰｕｓｅｄｏ　Ｈｅａｄｅｒを作成し、受け取ったＩＰパケットのＩＰヘッダと置き換え、ＴＣＰ／ＵＤＰ受信処理部３１５に受け渡すといったＩＰｖ６受信後処理を行なう。また、ＩＰ受信部３１４は、受信アクセス制御部３１６をさらに備える。
【００７０】
受信アクセス制御部３１６は、ＩＰｖ６受信前処理部３ＩＩから、ＡＨヘッダまたはＥＳＰヘッダを有していないＩＰパケットを受け取り、当該ＩＰパケットのアプリケーションへのアクセスを制御するものである。
【００７１】
ＳＡデータベース３０９は、ＩＰｓｅｃで必要なセキュリティアソシエーション（ＳＡ）が格納されているものである。
【００７２】
アクセスポリシデータベース３０８は、グループ内での通信を実現するため、各ノードに対するアクセス制御に関する情報及びグループ情報が格納されているものである。
【００７３】
アクセスポリシデータベース３０８は、グループ管理テーブル６００と、アクセス制御対象アプリケーション管理テーブル７００と、グループメンバ管理テーブル８００とを備える。
【００７４】
なお、グループ管理テーブル６００は、記憶媒体インタフェース２０６を介してノードに接続される記憶媒体であるメモリカード上でも保持されるものである。
【００７５】
以下、グループ管理処理部３０２、アクセスポリシデータベース３０６の各データベース、および、ＳＡデータベース３０９内のＳＡについて、その詳細を説明する。
【００７６】
図６に、グループ管理処理部３０２の機能構成図を示す。
【００７７】
本図に示すように、グループ管理処理部３０２は、制御部３１００と、グループ生成処理部３２００と、グループ参加処理部３３００と、グループ離脱処理部３４００と、グループ情報更新処理部３５００と、グループ制御ＩＰパケット受信処理部３６００とを備える。
【００７８】
グループ管理処理部３０２は、ユーザがメモリカードを記憶媒体インタフェース２０６に挿入したことを検出した記憶媒体インタフェース処理部３１８からの指示で処理を開始する。
【００７９】
制御部３１００は、記憶媒体インタフェース処理部３１８からの指示を受け、挿入されたメモリカード内と、自身が保有するアクセスポリシデータベース３０８を検索し、グループ管理テーブル６００の有無を確認する。
【００８０】
グループ生成処理部３２００は、グループ自体が存在しない場合に、新たにグループを生成するグループ生成処理を行なう。グループ生成処理は、制御部３１００がメモリカードにもアクセスポリシデータベース３０８にもグループ管理テーブル６００が存在しないと判断した場合に行なわれるものである。

【００８１】
具体的には、グループに属する他のノードと暗号通信を行なうために必要な情報、すなわち、グループ管理テーブル６００に登録すべき項目を生成、選択し、グループ管理テーブル６００を作成し、それを、メモリカードおよびアクセスポリシデータベース３０８に登録する。
【００８２】
グループ参加処理部３３００は、既存のグループに、新たなメンバとして自身を参加させるグループ参加処理を行うものである。グループ参加処理は、制御部３１００がメモリカードにはグループ管理テーブル６００が存在するが、アクセスポリシデータベース３０８にグループ管理テーブル６００が存在しないと判断した際に行われるものである。
【００８３】
グループ参加処理部３３００は、挿入されたメモリカードに格納されている暗号通信に必要な情報を取得し、また、自身のノード１００と暗号通信を行なうために必要な情報をグループに既に属している他のノード１００に送信する。具体的には、メモリカード内のグループ管理テーブル６００に自身の情報を追加し、自身の情報が追加されたグループ管理テーブル６００を、アクセスポリシデータベース３０８に登録する。
【００８４】
また、グループ管理テーブル６００から得た、グループに既に属しているノード１００のホスト名からＩＰアドレスを解決することで、グループメンバ管理テーブル８００を生成する。
【００８５】
さらに、グループ参加処理部３３００は、グループ内の各ノード１００とＩＰｓｅｃ通信が可能となるように、セキュリティアソシエーションの設定を行ない、ＳＡデータベース３０９に登録し、グループ内の既存のメンバのノード１００に、ＩＰｓｅｃ通信で自身が追加されたことを通知する。
【００８６】
グループ離脱処理部３４００は、グループから離脱するグループ離脱処理を行なうものである。
【００８７】
本実施形態では、ユーザが所定のノード１００をグループから離脱させたい場合、当該ノード１００に空のメモリカードを挿入することとする。すなわち、グループ離脱処理は、制御部３１００が、自身のアクセスポリシデータベース３０８にはグループ管理テーブル６００が存在するが、挿入されたメモリカードにはグループ管理テーブル６００が存在しないと判断した際に行われるものである。
【００８８】
グループ離脱処理は、グループに属する他のノード１００に自身のノード１００が離脱することを通知し、当該グループ内で暗号通信を行なうために必要な情報、すなわち、自身のアクセスポリシデータベース３０８およびＳＡデータベース３０９内のグループ間の通信に係わるデータを削除するものである。
【００８９】
ここで、グループ参加処理部３３００およびグループ離脱処理部３４００がそれぞれ、参加および離脱をグループに属する各ノード１００に通知する際は、グループ制御１Ｐパケットと呼ぶ特別なデータ部を有するＩＰパケットを用いる。
【００９０】
ここで、そのグループ制御ＩＰパケットについて説明する。図７にグループ制御１Ｐパケットのデータ部１０００の一例を示す。
【００９１】
本図に示すように、グループ制御ＩＰパケットのデータ部１０００は、コマンド識別子を格納するコマンド識別子格納部１００１と、ＩＰアドレスとホスト名とをそれぞれ格納する、１６バイトのＩＰアドレス格納部１００２と、ホスト名格納部１００３とを備える。

【００９２】
ここで、新規参加を通知する際にグループに属する各ノード１００に送信されるグループ制御ＩＰパケットの場合、コマンド識別子格納部１００１に「加入」を示す（００）ｈｅｘが設定される（以後、本グループ制御ＩＰパケットを加入コマンドと呼ぶ）。そして、ＩＰアドレス格納部１００２と、ホスト名格納部１００３とには、それぞれ自身のアドレスとホスト名とが設定される。
【００９３】
また、グループから離脱する際にグループに属する各ノード１００に送信されるグループ制御ＩＰパケットの場合、コマンド識別子格納部１００１に「離脱」を示す（０１）ｈｅｘが設定される（以後、本グループ制御ＩＰパケットを離脱コマンドと呼ぶ）。そして、ＩＰアドレス格納部１００２と、ホスト名格納部１００３とには、それぞれ自身のアドレスとホスト名とが設定される。
【００９４】
グループ情報更新処理部３５００は、グループ管理テーブル６００の内容を更新したり、それをメモリカードにコピーするといったグループ情報更新処理を行なうものである。
【００９５】
本実施形態においては、セキュリティを向上させるために、グループ内で利用するグループ鍵が所定の期間ごとに更新される設定となっている。グループ情報更新処理部３５００は、グループ管理テーブル６００の鍵有効期限がタイムアウトした時点で、新しいグループ鍵を生成する。
【００９６】
ここで、グループ管理テーブル６００生成時に、ノード毎に、異なる鍵有効期限が設定される。具体的には、所定の有効期限の、例えば、プラスマイナス３０％間のランダムな値を、その鍵有効期限に加算あるいは減算することで得られた値を鍵有効期限として各ノードに設定する。このため、各ノードで鍵有効期限のタイムアウトが異なるタイミングで生じ、鍵の更新を行なうノードが一つに定まり、グループのメンバが同時にグループ鍵を生成することを避けることができる。
【００９７】
そして、更新されたグループ鍵を更新前のグループ鍵で暗号化し、グループ鍵を更新したメンバからグループに属する各ノードに送付する。このとき、鍵の更新とともに、各ノードの鍵有効期限を再設定してもよい。
【００９８】
また、グループ情報更新処理部３５００は、他のノードから、更新されたグループ鍵を受信した場合、自身の保有するグループ鍵の情報を更新するとともに、グループに属する各ノード１００のＩＰアドレスが更新された場合、関連するデータベース内のＩＰアドレスを更新する。
【００９９】
ここで、本実施形態では、グループの鍵の更新は上述のように行なわれるため、グループ参加処理に用いられるメモリカード内のグループ管理テーブル６００には反映されない。同様に、上述のグループからの離脱処理は、空のメモリカードを用いて行なわれ、離脱したノード１００からグループを構成する他のノード１００への通知は、ＩＰｓｅｃ通信によって行われる。このため、グループ離脱によるグループ構成メンバの変更も、グループ参加処理に用いられるメモリカード内のグループ管理テーブル６００に反映されない。
【０１００】
このため、本実施形態では、グループ情報更新処理部３５００が、メモリカード内のグループ管理テーブル６００の更新処理も行なう。
【０１０１】
グループ情報更新処理部３５００が行なうメモリカード内のグループ管理テーブル６００の更新処理は、制御部３１００が、自身のアクセスポリシデータベース３０８にも、挿入されたメモリカードにもグループ管理テーブル６００が存在すると判断した際に行われる

ものである。

【０１０２】

グループ情報更新処理部３５００は、当該ノード１００のアクセスポリシデータベース３０８に格納されているグループ管理テーブル６００の情報をメモリカード内のグループ管理テーブル６００にコピーする。

【０１０３】

本実施形態では、実際のグループ参加処理において、グループ参加処理を行なう場合に、グループに既に所属しているノード１００にメモリカードを挿入し、メモリカード内のグループ管理テーブル６００を最新のものとする処理を前もって行なうよう手順を定めておく。

【０１０４】

グループ制御ＩＰパケット受信処理部３６００は、前述のグループ制御ＩＰパケットを受信した際の処理を行うものである。

【０１０５】

具体的には、加入コマンドを受信した場合は、ＩＰアドレス格納部１００２およびホスト名格納部１００３に格納されているＩＰアドレスおよびホスト名を自身のグループ管理テーブル６００およびグループメンバ管理テーブル８００とに追加し、送信元ノード１００と暗号通信を行なうために必要なセキュリティアソシエーションを作成する。一方、離脱コマンドを受信した場合は、それらを削除する。

【０１０６】

次に、アクセスポリシデータベース３０８に格納されるグループ管理テーブル６００とアクセス制御対応アプリケーション管理テーブル７００と、グループメンバ管理テーブル８００とについて以下に説明する。

【０１０７】

グループ管理テーブル６００は、グループに属するノード１００を識別するための情報とグループで共有する鍵の情報とを格納するテーブルである。図８にその一例を示す。

【０１０８】

本図に示すようにグループ管理テーブル６００は、ネットワークに接続されたノード１００によって構成されるグループを識別するためのグループ識別子を格納するグループ識別子格納フィールド６０１と、グループ鍵を格納するグループ鍵格納フィールド６０２と、そのグループ鍵の有効期限を格納するグループ鍵有効期限格納フィールド６０３と、ＡＨ、ＥＳＰといったグループ内で通信に利用するＩＰｓｅｃの機能の種別を格納するＩＰｓｅｃ種別格納フィールド６０４と、認証あるいは暗号に用いるアルゴリズムを格納するアルゴリズム格納フィールド６０５と、グループに属するノード１００を識別する情報であるホスト名を格納するホスト名格納フィールド６０６（６０６Ａ～６０６Ｂ）とを備える。

【０１０９】

アクセス制御対象アプリケーション管理テーブル７００は、ノード１００にグループ外のノード１００が利用可能なアプリケーションが実装されている場合、ノード１００に実装されている各アプリケーションに対するアクセス制御のために用いる情報が格納されているテーブルである。

【０１１０】

なお、本テーブルは、ノード１００がグループ内からのアクセスに対してのみ提供するアプリケーションだけを実装している場合は不要なものである。

【０１１１】

アクセス制御対象アプリケーション管理テーブル７００の一例を図９に示す。

【０１１２】

本図に示すように、アクセス制御対象アプリケーション管理テーブル７００は、グループ外のノード１００にも開放されているアプリケーションが利用するポート番号を格納するポート番号格納フィールド７０１（７０１Ａ、７０１Ｂ）を備える。各ノード１００は、

ＩＰパケット受信時に、本テーブルを参照し、当該ＩＰパケットがアクセスしようとしているアプリケーションがグループ外のノード１００にも開放されたアプリケーションであるか否かの判定を行う。

【０１１３】

次に、グループメンバ管理テーブル８００について説明する。各ノード１００間で、ＩＰｖ６に基づき、１Ｐパケット通信を行なうためには、各ノード１００のＩＰアドレスを知る必要がある。グループに属する各ノード１００の１ＰアドレスはＬ、グループ参加時に取得した各ノード１００のホスト名からＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ） Ｅｃｈｏ Ｒｅｑｕｅｓｔ／Ｒｅｐｌｙパケットのやりとりにより、アドレスの解決を行なうことで取得する。このように、グループメンバ管理テーブル８００は、各ノードにおいてホスト名からＩＰアドレスを解決して作成するもので、そこには、グループに属する各ノード１００のホスト名とＩＰアドレスとの対応が格納されている。

【０１１４】

図１０にグループメンバ管理テーブル８００の一例を示す。

【０１１５】

本図に示すように、本テーブルは、ノードを特定するホスト名を格納するホスト名格納フィールド８０１と、ホスト名と対応させて各ノード１００のＩＰアドレスを格納するＩＰアドレス格納フィールド８０２と、ＩＰアドレスの有効期限を格納する有効期限格納フィールド８０２とを備える。

【０１１６】

ノード１００が再起動した場合などに、ノード１００のＩＰアドレスは変わる可能性がある。また、一定時間内にＩＰアドレス格納部８０２に格納されているＩＰアドレスと送受信が行われないと、有効期限が切れる場合がある。

【０１１７】

このようなノードに対しＩＰパケットを送信する場合、ノード１００のＩＰｖ６送信前処理部３０５は、ＩＣＭＰ Ｅｃｈｏ Ｒｅｑｕｅｓｔ／Ｒｅｐｌｙパケットのやりとりにより、ホスト名からアドレスの解決を再度行ない、グループ管理処理部３０２に通知する。それを受けて、グループ管理処理部３０２のグループ情報更新処理部３５００は、ＩＰアドレスが登録されている本テーブルおよびグループ内の通信に利用するセキュリティアソシエーションを更新する。

【０１１８】

次に、ＳＡデータベース３０９に格納されている、セキュリティアソシエーション９００について説明する。セキュリティアソシエーション９００は、１Ｐｓｅｃにのっとった通信を行うために共有すべき情報を管理するものであり、例えば、ノード１００Ａとノード１００Ｂ間で通信する場合、ノード１００Ａからノード１００Ｂ方向の通信、および、ノード１００Ｂからノード１００Ａ方向の通信、両者に対し、独立して設定する必要があるものである。

【０１１９】

図１１に、セキュリティアソシエーション９００の一例を示す。

【０１２０】

本図に示すように、セキュリティアソシエーション９００は、各セキュリティアソシエーションを識別するＳＰＩ（セキュリティポリシ識別子）、送信元ＩＰアドレス、送信先アドレス、プロトコルとして認証あるいは暗号の指定、暗号範囲としてトランスポートモードあるいはトンネルモードの指定、暗号アルゴリズム、暗号鍵、認証アルゴリズム、認証鍵、鍵の有効期限などを含む。

【０１２１】

本実施形態では、各ノード１００においてセキュリティアソシエーション９００を作成するにあたり、送信用のセキュリティアソシエーション９００を作成する場合は、送信元ＩＰアドレスには、自身のノードＩ００のＩＰアドレスを、送信先ＩＰアドレスには、通信

相手先ノードのＩＰアドレスを設定し、受信用を作成する場合は、送信元ＩＰアドレスには、通信相手先のＩＰアドレスを設定し、送信先ＩＰアドレスには、自身のノード１００のＩＰアドレスを設定する。

【０１２２】

ＳＰＩには、送信用、受信用ともに、グループ管理テーブル６００のグループ識別子格納部６０１に格納されているグループ識別子が格納される。また、送信用、受信用ともに、プロトコル、認証鍵アルゴリズム、認証鍵、有効期限には、それぞれ、グループ管理テーブル６００に格納されているものが設定される。

【０１２３】

以上、本実施形態におけるノード１００の各機能などについて説明した。

【０１２４】

次に、本実施形態における、ネットワーク１１０に接続された各ノード１００間で、グループを生成し、参加する手順、また、一旦参加したグループから離脱する手順などを説明する。

【０１２５】

以下においては、ＩＰｓｅｃの機能種別としてＡＨを、モードとしてトランスポートモードを、認証アルゴリズムとしてＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １：ＳＨＳ（Ｓｅｃｕｒｅ Ｈａｓｈ Ｓｔａｎｄａｒｄ） ＦＩＰＳ １８０として規定）を用いる場合を例にあげ、説明する。ＩＰｓｅｃ通信の設定は、これらに限られない。

【０１２６】

また、本実施形態においては、前述したように、グループの情報を格納するメモリカードと、グループを離脱する際に用いる空のメモリカードとの２つのメモリカードを用いてグループの生成、参加、離脱、情報更新などを行なう。

【０１２７】

図１２に、グループ管理処理部３０２が行なうグループ管理処理手順３０２０を示す。

【０１２８】

グループ管理処理手順３０２０は、ユーザがメモリカードを各ノード１００の記録媒体インタフェース２０６に挿入することをきっかけに開始される。

【０１２９】

そして、ノード１００の記憶媒体インタフェース処理部３１８は、メモリカードが記録媒体インタフェース２０６に挿入されたことを検出すると、記憶媒体インタフェース２０６に備えられているＬＥＤライトを点灯し、メモリカードを利用中であることを利用者に対して示す。

【０１３０】

ＬＥＤライトが消灯されたことにより、ユーザは処理が終了したことを知り、メモリカードを取り出すことができる。

【０１３１】

また、記憶媒体インタフェース処理部３１８は、メモリカードを検出したことをグループ管理処理部３０２へ通知する。その通知を受けて、グループ管理処理部３０２は、グループ管理処理１０００を開始する。

【０１３２】

まず、グループ管理処理部３０２の制御部３１００は、自身のアクセスポリシデータベース３０８と、記録媒体インタフェース処理部３１８を介してメモリカード挿入されたメモリカードとにアクセスし、グループ管理テーブル６００の有無を確認する（ステップ３０２１）。

【０１３３】

ここで、どちらにもグループ管理テーブル６００がない場合、グループ自体が存在しない、すなわち、グループを生成する必要があると判断し、制御部３１００は、グループ生成処理部３２００にグループ生成処理３２１０を行わせる（ステップ３０２２）。グループ

生成処理３２１０が完了すると、制御部３０２は、記憶媒体インタフェース処理部３１８に対し、メモリカードの書き込み終了を通知し（ステップ３０２７）、処理を終える。自身のアクセスポリシデータベース３０２には無く、メモリカードには存在した場合、制御部３１００は、メモリカードに存在するグループに自身が参加しようとしていると判断し、グループ参加処理部３３００にグループ参加処理３３１０を行なわせ（ステップ３０２３）、グループ参加処理が完了すると、ステップ３０２７に進む。

【０１３４】

メモリカードには無く、自身のアクセスポリシデータベース３０２には存在した場合、制御部３１００は、自身は既にグループに属しているが空白のメモリカードが挿入されたことにより、グループ離脱処理を行なうものと判断し、グループ離脱処理部３４００にグループ離脱処理３４１０を行なわせ（ステップ３０２６）、グループ離脱処理が完了するとステップ３０２７に進む。

【０１３５】

どちらにもグループ管理テーブル６００が存在する場合は、制御部３１００は、まず、アクセスポリシデータベース３０２内のグループ管理テーブル６００とメモリカード内のグループ管理テーブル６００とのグループ識別子を比較する（ステップ３０２４）。

【０１３６】

ここで、両者が同じであれば、メモリカードのグループ情報を更新する処理を行なうものと判断し、グループ情報更新処理部３５００にグループ情報更新処理３５１０としてアクセスポリシデータベース３０２内のグループ管理テーブル６００をメモリカードにコピーする処理を行なわせ（ステップ３０２５）、当該処理が完了すると、ステップ３０２７に進む。

【０１３７】

ステップ３０２４において、両者が異なった場合、制御部３１００は、誤ったメモリカードが挿入されたと判断し、そのままステップ３０２７にすすむ。

【０１３８】

次に、グループ生成処理１２００、グループ参加処理１３００、グループ離脱処理１６００、グループ情報更新処理１５００の手順を説明する。

【０１３９】

まず、グループ生成処理３２１０の処理手順を図１３に示す。

【０１４０】

制御部３１００から処理開始の指示を受けると、グループ生成処理部３２００は、グループ鍵を生成し（ステップ３２１１）、グループを識別するためのグループ識別子を生成し（ステップ３２１２）、認証・暗号モードとして認証（ＡＨ）を選択し（ステップ３２１３）、アルゴリズムとしてＳＨＡ－１を選択する（ステップ３２１４）。

【０１４１】

そして、それぞれを、グループ鍵格納フィールド６０２、グループ識別子格納フィールド６０１、ＩＰｓｅｃ種別格納フィールド６０４、アルゴリズム格納フィールド６０５に格納し、グループ管理テーブル６００を作成する（ステップ３２１５）。そして、ホスト名格納フィールド６０６に自ノード１００のホスト名を登録する（ステップ３２１６）。

【０１４２】

グループ管理テーブル６００が完成すると、グループ生成処理部３２００は、本テーブルをメモリカードにコピーすると共に、自ノード１００のアクセスポリシデータベース３０８に記憶し（ステップ３２１７，３２１８）、処理が終了したことを制御部３１００に通知する。

【０１４３】

次に、グループ参加処理３３１０の処理手順を図１４に示す。

【０１４４】

制御部３１００から処理開始の指示を受けると、グループ参加処理部３３００は、メモリカード上のグループ管理テーブル６００のホスト名格納フィールド６０６に自ノード１０

０のホスト名を追加し（ステップ３３１１）、メモリカード上のグループ管理テーブル６００を自身のアクセスポリシデータベース３０８内に記憶する（ステップ３３１２）。

【０１４５】

次に、グループメンバ管理テーブル８００を作成するとともに、グループに既に属している各ノード１００に、自身の参加を通知する新メンバ通知処理３７１０を行なう（ステップ３３１３）。

【０１４６】

そして、今までのステップで記録されたグループ管理テーブル６００の情報およびグループメンバ管理テーブル８００の情報とを用い、各ノード１００とのＩＰｓｅｃ通信に用いるセキュリティアソシエーション９００を生成し（ステップ３３１４）、処理が終了したことを制御部３１００に通知する。

【０１４７】

ここで、新メンバ通知処理３７１０についてその処理手順を説明する。図１５にその処理手順を示す。

【０１４８】

新メンバ通知処理３７１０では、グループ管理テーブル６００内のホスト名フィールド６０６に格納されているホストごとに順に、ＩＣＭＰ Ｅｃｈｏ Ｒｅｑｕｅｓｔ／Ｒｅｐｌｙによりアドレスを取得し（ステップ３７１２）、グループメンバ管理テーブル８００に、ホスト名ごとに取得したＩＰアドレスを登録する（ステップ３７１３）。

【０１４９】

上記のステップで取得した、グループを構成する各ノード１００のＩＰアドレスに対して加入コマンドを生成し（ステップ３７１４）、それを送信する（ステップ３７１５）。

【０１５０】

そして、次のホスト名を読み出して、ステップ１３３０から１３６０の処理を繰り返す（ステップ３３１６）。ここで、読み出したホスト名が自身のホスト名の場合は、何も処理を行わず、次のホスト名を読み出す（ステップ３７１１）。そして、グループ管理テーブル６００のホスト名格納フィールド６０６に格納されている、自身のノード１００を除く全てのノードに対して以上の処理を終えると（ステップ３７１７）、グループ内への新メンバ通知処理１３３０を終える。

【０１５１】

以上、グループ参加処理３３１０について説明した。

【０１５２】

次に、グループ離脱処理３４１０について、図１６を用いて説明する。

【０１５３】

制御部３１００から処理開始の指示を受けると、グループ離脱処理部３４００は、ノード１００内のグループ管理テーブル６００のホスト名格納部６０６に登録されているホスト名を順番に読み出す（ステップ３３１１）。

【０１５４】

ここで、読み出したホスト名が自ホスト名と一致した場合は、次のホスト名を読み出す。

【０１５５】

読み出したホスト名が自ホスト名と一致しない場合は、グループメンバ管理テーブル８００から読み出したホスト名に対応するＩＰアドレスを検索する（ステップ３３１２）。以後、このＩＰアドレスを検索したＩＰアドレスと呼ぶ。

【０１５６】

次に、送信先ＩＰアドレスを検索したＩＰアドレスとした離脱コマンドを作成し（ステップ３３１３）、その送信先ＩＰアドレスを有するノード１００に送信する（ステップ３３１４）。

【０１５７】

グループ離脱処理部３４００は、自身の保有するグループメンバ管理テーブル８００から以上の操作を行なった検索したＩＰアドレスに係わるデータを削除する（ステップ３３１

５）。

【０１５８】

次に、ＳＡデータベース３０９に記憶されているセキュリティアソシエーション９００から検索したＩＰアドレスと等しい送信先ＩＰアドレスを持つものを抽出し、そのセキュリティアソシエーション９００を削除する（ステップ３３１６）。

【０１５９】

また、検索した１ＰアドレスとＩＰアドレスを持つセキュリティアソシエーション９００を抽出し、それを削除する（ステップ３３１７）。

【０１６０】

グループ離脱処理部３４００は、グループ管理テーブル６００に登録されている全てのホスト名に対して、以上のステップ３３１１～ステップ３３１７の処理を実行した後（ステップ３３１８）、自身が保有するグループ管理テーブル６００を削除し（ステップ３３１９）、グループ離脱処理３３１０を終了する。そして、制御部３１００に処理終了を通知する。

【０１６１】

次に、上記のグループ参加処理３３１０内のグループ内への新メンバ通知処理３７１０のステップ３７１５およびグループ離脱処理３３１０のステップ３３１４において送信された、それぞれ加入コマンドおよび離脱コマンドを受信した場合の各ノード１００側での処理を以下に説明する。

【０１６２】

本処理は、グループ制御１Ｐパケット受信処理部３６００によって行なわれ、グループ制御ＩＰパケット受信処理３６１０と呼ぶ。図１７に本処理の手順を示す。

【０１６３】

グループを構成する各ノード１００は、ネットワークインタフェース受信処理部３１０においてグループ制御ＩＰパケットを受信すると、ＩＰ受信部３１４、ＴＣＰ／ＵＤＰ受信処理部３１５を経てグループ管理処理部３０２のグループ制御ＩＰパケット受信処理部３６００へ受け渡す。

【０１６４】

受信したグループ制御１ＰパケットＩＰ受信処理部３６００は、コマンド識別子格納部１００１に設定されているコマンド識別子が加入であるか否かを確認する（ステップ３６１１）。

【０１６５】

ステップ３６１１でコマンド識別子が加入を示す（００）ｈｅｘであった場合、すなわち、加入コマンドを受信した場合、ステップ３６１２に進み、グループ制御ＩＰパケットのホスト名１００３に設定されている加入コマンドを送信してきたノード１００のホスト名をグループ管理テーブル６００に登録する（ステップ３６１２）。

【０１６６】

そして、グループメンバ管理テーブル８００に、加入コマンドを送信してきたノード１００のホスト名と、グループ制御ＩＰパケットのＩＰアドレス格納部１００２に設定されているそのＩＰアドレスとを登録する（ステップ３６１３）。

【０１６７】

次に、グループ制御１ＰパケットＩＰ受信処理部３６００は、送信用、すなわち、自身のノード１００から加入コマンドを送信してきた新規に加入したノード１００方向の送信、および、受信用、すなわち、加入コマンドを送信してきた新規に加入したノード１００から自身のノード１００方向の送信、各々のセキュリティアソシエーション９００を作成する処理を行なう（ステップ３６１４、３６１５）。

【０１６８】

次に、ステップ３６１１でコマンド識別子が離脱を示す（０１）ｈｅｘであった場合、すなわち、離脱コマンドを受信した場合、グループ制御ＩＰパケット受信処理部３６００は、ステップ３６１６に進む。

【０１６９】
ここで、グループ制御ＩＰパケット受信処理部３６００は、ＳＡデータベース３０９に記憶されているセキュリティアソシエーション９００から、受信したグループ離脱コマンドのデータ部１０００のＩＰアドレス１００２に格納されているＩＰアドレスと等しい送信先１ＰアドレスをＩＰを持つものを抽出し、抽出したセキュリティアソシエーションを削除する（ステップ３６１６）。
次に、受信した離脱コマンドのＩＰアドレス１００２と等しいＩＰアドレスを有するデータをグループメンバ管理テーブル８００から削除し（ステップ３６１７）、受信した離脱コマンドのホスト名１００３に格納されているホスト名と等しいホスト名を、自ノード１００上のグループ管理テーブル６００から削除する（ステップ３６１８）。
【０１７０】
グループ内の全てのノード１００において以上の手順を行なうことにより、全てのノード１００が保有する離脱したノード１００に対応するセキュリティアソシエーション９００を削除し、また、グループ管理テーブル６００から、離脱したノード１００の情報を削除する。
【０１７１】
以上のようにして、グループを構成するノード１００に新規加入または離脱といった変更があった場合、当該ノード１００から送信されるグループ制御ＩＰパケットを受信した他のノード１００において、自身の保有するセキュリティアソシエーションおよびグループ管理テーブル６００が更新される。
【０１７２】
以上、グループ制御ＩＰパケット受信処理を説明した。
【０１７３】
ここまで、グループ管理処理部３０２による、グループの生成、参加、離脱などのグループ管理処理について説明した。
【０１７４】
次に、上記の手順で生成され管理されているグループ内で、アプリケーションを互いに利用する手順を以下に説明する。
【０１７５】
アプリケーションの利用は、ＩＰパケットを互いに送受することによって行なわれる。まず、このＩＰパケットの送受信について説明する。
【０１７６】
前述のように、ＩＰｓｅｃ通信を行うために予め設定の必要なセキュリティアソシエーション９００は、グループ管理処理３０２において、新たなグループ構成メンバが追加される際に生成される。すなわち、グループに属している限り、ＩＰｓｅｃ通信は可能である。
【０１７７】
ＩＰパケットを送信するにあたり、ＩＰｓｅｃ送信処理部３０６は、送信するＩＰヘッダの送信先ＩＰアドレスをキーに、ＳＡデータベース３０９を検索し、対応するＩＰアドレスが送信先ＩＰアドレスとして格納されているセキュリティアソシエーション９００を抽出する。抽出したセキュリティアソシエーション９００に登録されている情報に基づき、ＩＰｓｅｃ処理を行い、ＩＰｖ６送信後処理３０７を行い、ネットワークインタフェース送信処理部を介して、送信先ノードにＩＰパケットを送信する。
【０１７８】
次に、ＩＰパケット受信時の処理手順を図１８を用いて説明する。
【０１７９】
ネットワークインタフェース受信処理部３１０を介してＩＰパケットを受信すると、ＩＰｖ６受信前処理部３１１は、ＩＰｖ６受信前処理を行い（ステップ４０１０）、受信したＩＰヘッダ内の、ＡＨヘッダの有無をチェックする（ステップ４０２０）。
【０１８０】

受信したＩＰヘッダ内にＡＨヘッダ４０１があると判断したならば、そのＩＰパケットをＩＰｓｅｃ受信処理部３１２に受け渡す。

【０１８１】

受け取ったＩＰｓｅｃ受信処理部３１２は、後述するＩＰｓｅｃ受信処理３１２０を行い（ステップ４０３０）、ＩＰｖ６受信後処理部３１３にＩＰパケットを受け渡す。

【０１８２】

そして、ＩＰｖ６受信後処理部３１３は、ＩＰｖ６受信後処理３１３０を行い（ステップ４０４０）、処理を終了する。

【０１８３】

なお、ここで、ＩＰｖ６受信後処理部３１３は、ＩＰｖ６受信後処理３１３０を終えた受信したパケットをＴＣＰ／ＵＤＰ受信処理部３１５に受け渡す。受け取ったＴＣＰ／ＵＤＰ受信処理部３１５は、受け取ったパケットの受信処理を行い、アプリケーション３０１に受信データとして渡す。

【０１８４】

ステップ４０２０で、上記のヘッダがないと判断した場合、そのＩＰパケットを受信アクセス制御部３１６に受け渡す。

【０１８５】

受け取った受信アクセス制御部３１６は、それがＩＣＭＰパケットであるか否かチェックする（ステップ４０５０）。

【０１８６】

ステップ４０５０で、受信したＩＰパケットが、ＩＣＭＰパケットであると判断されたならば、そのままＩＰｖ６受信後処理部３１３に受け渡し、ＩＰｖ６受信後処理３１３０を行い（ステップ４０４０）、処理を終了する。

【０１８７】

ステップ４０５０で、ＩＣＭＰパケットではないと判断されたならば、受信アクセス制御部３１６は、そのＩＰパケットをグループ外のノード１００から送信されたグループ外ＩＰパケットであると判断し、後述するグループ外ＩＰパケット受信処理３１６０を行い（ステップ４０６０）、処理を終了する。

【０１８８】

次に、上記のＩＰｓｅｃ処理３１２０について説明する。

【０１８９】

ＩＰｓｅｃ処理部３１２は、ＡＨヘッダを有するＩＰパケットを受信すると、ＩＰヘッダの送信元ＩＰアドレス、送信先ＩＰアドレス、ＡＨヘッダ４０１に設定されているＳＰＩが一致するセキュリティアソシエーション９００をＳＡデータベース３０９から抽出する。

【０１９０】

そして、抽出したセキュリティアソシエーション９００に記憶されている認証鍵を用いて受信したＩＰパケットの認証情報を作成し、ＡＨヘッダ４０１に設定されている認証情報と比較する。

【０１９１】

両者が一致していれば、受信したＩＰパケットをグループに属する正当なノード１００からの送信とみなし、ＩＰｖ６受信後処理部３１３に受け渡す。そして、一致しない場合は、そのＩＰパケット破棄する。

【０１９２】

以上ＩＰｓｅｃ処理３１２０について説明した。

【０１９３】

次に、受信アクセス制御部３１６によるグループ外パケット受信処理３１６０について説明する。

【０１９４】

以上のように、本実施形態においては、グループに属するノード１００は、グループ外の

ノードＩ００から、ＡＨヘッダを有するＩＰパケットを受信した場合は、ＩＰｓｅｃ通信処理部３１２において、また、ＡＨヘッダを有しないＩＰパケットを受信した場合は、ＩＰｖ６受信前処理部３１１において、当該ＩＰパケットが、ＩＰｖ６受信後処理部３１３、ＴＣＰ／ＵＤＰ受信処理部３１５を介してアプリケーション３０１に到達することを排除している。

【０１９５】

しかし、本実施形態においては、ノード１００によっては、その保有するアプリケーションの利用を、グループ外のノード１００にも開放しているものがある。前述したように、このようなアプリケーションを有するノード１００は、アプリケーションごとのポート番号を、アクセス制御対象アプリケーション管理テーブル７００において管理している。

【０１９６】

グループ外のノード１００からＡＨヘッダを有するＩＰパケットを受信した場合は、そのＩＰパケットを復号することができないため、それはＩＰｓｅｃ通信処理部３１２において破棄することは先に説明した。

【０１９７】

グループ外ＩＰパケット受信処理３１６０は、グループ外のノード１００から通常のＩＰパケットを受信した際に、グループ外のノード１００に開放しているアプリケーションに当該ＩＰパケットを送達する処理である。

【０１９８】

グループ外ＩＰパケット受信処理３１６０では、ＩＰパケットを受け取ったノード１００が、グループ外のノード１００に対し何らサービス機能を提供しない場合、アクセスエラーをデータとして格納したＩＰパケットを送信元に対して送信し、受信したＩＰパケットは破棄する。これに対し、グループ外のノード１００に対して何らかのサービス機能を提供する場合は、アクセス制御対象アプリケーション管理テーブル７００の登録に従って、アプリケーションを提供するよう制御している。

【０１９９】

以下にその手順を図１９を用いて説明する。

【０２００】

受信アクセス制御部３１６は、ＩＰｖ６受信前処理部３１１からＩＣＭＰパケットではないＩＰパケットを受信した場合、当該ＩＰパケットから読取った送信先ポート番号とアクセス制御対象アプリケーション管理テーブル７００に登録されているポート番号７０１との比較を行なう（ステップ３１６１）。

【０２０１】

アクセス制御対象アプリケーション管理テーブル７００には、グループ外のノードに利用が許可されているアプリケーションのポート番号が登録されているため、両者が一致した場合、サービス機能を要求元ノードＩ００に提供できることとなる。

【０２０２】

この場合、受信アクセス制御部３１６は、受け取ったＩＰパケットをＩＰｖ６受信後処理部３１３に受け渡し、受け取ったＩＰｖ６受信後処理部３１３は、ＩＰｖ６受信後処理３１３０を行なう（ステップ３１６４）。

【０２０３】

そして、ＩＰｖ６受信後処理部３１３から処理されたＩＰパケットを受け取ったＴＣＰ／ＵＤＰ受信処理部３１５は、それを、アプリケーション３０１に受け渡す。

【０２０４】

ステップ３１６１において、ポート番号が一致しない場合は、提供できるサービス機能がないため、受信アクセス制御部３１６は、アクセスエラーをデータとして格納したＩＰパケットを生成しＩＰ送信部３０４から送信元に送信し（ステップ３１６２）、受信したＩＰパケットは破棄する（ステップ３１６３）。

【０２０５】

以上、グループ外ＩＰパケット受信処理について説明した。

【０２０６】
このように、本実施形態においては、グループ内のノード１００間ではＩＰｓｅｃ通信を行い、グループ外のノード１００とは通常のＩＰパケットによる通信を行うことで、アクセス制御対象アプリケーション管理テーブル７００で管理している各アプリケーションのポート番号に従って、アプリケーションごとにグループ内外のアクセス許可を制御することができる。これにより、一つのノード１００において、グループだけで利用するサービス機能と、誰もが利用できるサービス機能とを実装し、それぞれへのアクセス制御を可能としている。
【０２０７】
本実施形態によれば、ホームネットワークを構成するノード１００において作成したグループ鍵を含むＩＰｓｅｃ通信に必要な情報を、共通のメモリカードを介して、利用者が相互に利用することを許可する各ノード１００に配布する。
【０２０８】
配布されたノード１００は、グループに所属している他のノード１００とＩＰｓｅｃ通信ができるように、セキュリティアソシエーション９００を設定するとともに、新規加入したことを、グループに所属している他のノード１００に通知する。
【０２０９】
通知を受けたノード１００は、それぞれ、新規に加入したノード１００とのＩＰｓｅｃ通信ができるように、セキュリティアソシエーション９００を設定する。
【０２１０】
以上のように、本実施形態では、例えば、通信を開始する際に認証サーバ、あるいは鍵管理手段を備えた装置等といったグループを構成する機器以外の装置を介さずに、互いに認証可能で安全な通信を行なうことのできるグループを、そのグループを構成する機器が、容易に生成し管理することを実現している。
【０２１１】
また、グループを生成し管理するために必要な情報を、メモリカードといった記憶媒体を介して各ノードに与えること、および、グループの生成、グループへの参加、および、グループからの離脱の指示を各ノードに与えることを実現している。
【０２１２】
このように、本実施形態では、サーバなどの特別な機器を設けることなく、また、複数のマスタ鍵などを備えたＩＣカードを用意してグループを構成する機器それぞれに予めセットしておくなどの事前の準備をすることなく、グループを構成する機器間でのみ、容易にＩＰｓｅｃ通信可能な環境を構築できる。
【０２１３】
また、本実施形態では、一つのノードに、グループ内のノードのみ利用できるアプリケーションとグループ外のノードも利用できるアプリケーションとが実装されている場合も容易にそれぞれのアクセス制御を実現できる。
【０２１４】
なお、本実施形態では、グループ生成、加入、離脱時の指示を行なう際に利用する記憶媒体としてメモリカードを例にあげ、説明したが、利用する記憶媒体はこれに限られない。可搬型の記憶媒体であり、各ノードがそのインタフェースを備えていれば、どのような記憶媒体であってもよい。
【０２１５】
また、本実施形態では、ＩＰｓｅｃ通信を行うために必要な情報の授受を記憶媒体で行なうといった設定としたが、これに限られない。例えば、各ノードに入力装置を備え、ユーザが入力するようにしてもよい。
【０２１６】
さらに、グループからの離脱処理を開始するきっかけとして、空のメモリカードの入力を例にあげ説明したが、これに限られない。例えば、各ノードがリセットボタンを備え、ユーザがそのリセットボタンを介して離脱処理を開始する指示を与えるようにしてもよい。

【０２１７】
また、ＬＥＤを備えることにより、利用者に対しグループ生成、加入処理の終了を通知する事を実現している。通知のための機能も、これに限られない。
【０２１８】
なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。
【０２１９】
例えば、上記の実施形態では、宅内のネットワークを例にとり説明したが、本発明はこれに限定されない。本発明は、互いに認証を必要とする様々なネットワークシステムに広く適用できる。
【０２２０】
次に、上述した実施形態に基づきノードの管理者が認識している範囲での利用対象であるノードＡからノードＦでグループにおいて、利用者対応に利用できるノードを制限するサブグループの実施形態について、図２０から図３１を参照し説明する。
【０２２１】
図２０は、本発明を適用した宅内ネットワーク、ＳＯＨＯと言ったスモールオフィスネットワーク、オフィスのフロアネットワークを代表とするようなローカルなネットワークの一構成例を示す。本発明では、以下、宅内において本発明を適用した場合を例として説明する。宅内ネットワークは、複数のノード１０５（１０５Ａ、Ｂ）、１０６（１０６Ｃ～Ｆ）、例えば電子レンジやエアコンなどの家電機器、テレビやビデオなどのＡＶ機器、センサ等、及びＰＣから構成され、各機器はＩＰｖ６によりＩＰパケットの送受信が可能であるとする。本ネットワークは、ノード１０５、１０６、各々が備えるサービス機能の他ノード１０５、１０６からの操作、あるいは他ノード１０５、１０６へのサービス提供を実現するものである。
【０２２２】
また、これら複数のノード１０５、１０６は、上述の実施形態に基づきグループ共通のグループ鍵６０２を用いたＩＰｓｅｃ通信が可能なＳＡ９００が各ノードに設定され、グループ間の通信には、前記グループ鍵６０２を用いたＩＰｓｅｃ通信が行える状態となる。以下、本グループをルートグループ１０７と呼ぶ。ルートグループ１０７が構築されると、ルートグループ１０７を構成する全てのノード１０５、１０６において、グループアクセスデータベース３０８上のグループ管理テーブル６００及びＳＡデータベース３０９上にルートグループ１０７の全ノード１０５、１０６に対する送信用ＳＡ９００及び受信用ＳＡ９００が設定される。尚、本実施形態では、ルートグループにおけるグループ間通信に利用するＩＰｓｅｃ通信では、３ＤＥＳによる暗号化を適用するとする。
【０２２３】
本実施形態では、ノードが備えるユーザインタフェース機能により、ネットワーク機器を二つに大別する。第一のノード１０５は、ＰＣが備えるインタフェース機能、例えば宅内ネットワークを構成するノードのホスト名一覧が表示できるディスプレイ、文字入力が可能なキーボードを備えるノードである。第二のノード１０６はノードが本来備える機能を操作するための最低限のインタフェースを備えたノードである。第一のノード１０５に相当する機器としては、ＰＣ、テレビ、家電制御リモコン等を想定しており、図２０ではノードＡ１０５ＡとノードＢ１０５Ｂを第一のノード１０５とし、第二のネットワーク機器１０６に相当する機器としては、エアコン、電子レンジと言った白物家電及びセンサ等を想定し、図２０ではノードＣ１０６ＣからノードＦ１０６Ｆを第二のノードとしている。図２１に第一のノード１０５のハードウェア構成を示す。
【０２２４】
ノード１０５が備える一つ以上のノード固有機能部２０２、例えばエアコンであれば、例えば冷暖房機能、温度管理機能、タイマ機能等を司る処理部、ネットワークカード２０５、固有機能部及びネットワークカードを制御するプロセッサ２００、プロセッサで実行するプログラム及びユーザアクセス制御を備えたグループ通信を実現するグループアクセス

データベース３０８及びＳＡデータベース３０９を記憶するメモリ２０１、ユーザインタフェースの為のディスプレイを接続するデータ出力インタフェース部２０８とキーボードを接続するデータ入力インタフェース部２０９、メモリカード２０７等のインタフェースを提供する記憶媒体インタフェース２０６、及びこれらを接続するシステムバス２０３から構成される。前記記憶媒体インタフェース２０６は、挿入する記憶媒体の書き込み中をユーザに通知するＬＥＤ（発光ダイオード）ライトを具備しており、ＬＥＤライトの点燈により、ユーザに対し、書き込み中あるいは処理中を示す。第二のノード１０６のハードウェア構成は、前記第一のノード１０５のハードウェア構成から、ユーザインタフェースの為に利用するデータ出力インタフェース部２０８及びデータ入力インタフェース部２０９がない。

【０２２５】

図２０に第一のノード１０５のソフトウェア構成を示す。

ネットワークを介してグループ構成機器間でサービス提供する一つ以上のアプリケーションプログラム３０１、通信を実現するＴＣＰ／ＵＤＰ送信処理部３０３、ＩＰ送信部３０４、ネットワークカードを制御するネットワークインタフェース送信処理部３１７、ネットワークインタフェース受信処理部３１０、ＩＰ受信部３１１、ＴＣＰ／ＵＤＰ受信処理部３１５、ＩＰｓｅｃのセキュリティアソシエーション（以下ＳＡ）９００を管理するＳＡデータベース３０９、グループ通信を実現するために利用するネットワーク機器に対するアクセス制御に関する情報及びグループ情報を管理するアクセスポリシデータベース３０８、グループ管理を行うグループ管理処理部３０２、記憶媒体インタフェースを制御する記憶媒体インタフェース処理部３１８、及びデータ出力インタフェース部とデータ入力インタフェース部を制御するユーザインタフェース処理部１５１とから構成する。ＩＰ送信部３０４は、ＴＣＰ／ＵＤＰ送信処理部３０３が作成したＰｓｅｕｄｏヘッダからＩＰヘッダを作成するＩＰｖ６送信前処理部３０５、ＳＡ９００の有無を調べＳＡ９００がある場合にはＩＰｓｅｃ処理を行うＩＰｓｅｃ送信処理部３０６、ネットワークインタフェース送信処理部３１７へＩＰパケットを渡すＩＰｖ６送信後処理部３０７から構成され、ＩＰ受信部３１４は、ネットワークインタフェース受信処理部３１０から受信したＩＰパケットヘッダからペイロード長と受信データ長の比較、ヘッダオプションの処理を行うＩＰｖ６受信前処理３１１、ＡＨヘッダ、ＥＳＰヘッダがある場合にＳＡ９００を検索し、認証あるいは復号処理を行うＩＰｓｅｃ受信処理部３１２、ＡＨヘッダ、ＥＳＰヘッダが無い場合にＩＰパケットを受信するかどうかを判断する受信アクセス制御部３１６、ＩＰヘッダをＰｓｅｕｄｏヘッダに置き換え、ＴＣＰ／ＵＤＰ送信処理部３１５へ受信データを渡すＩＰｖ６受信後処理部３１３から構成する。

【０２２６】

グループ管理処理部３０２は、上述した実施形態に基づき、ルートグループ生成処理３２００、参加処理３３００、離脱処理３４００、情報更新処理３５００、グループ制御ＩＰパケット受信処理３６００に加えて、ユーザからのアクセス制御設定要求を受け付けるユーザアクセス制御処理２１００、及び他のネットワーク機器からのサブグループ管理に関するコマンド受信に対する処理を行うサブグループ管理処理２２００を行うとする。

【０２２７】

グループアクセスデータベース３０８として、グループ管理テーブル６００、アクセスユーザ管理テーブル２００１、及びアクセスアプリ管理テーブル２００３を配置する。

【０２２８】

ＳＡデータベース３０９として、ＩＰｓｅｃ通信を実現するための送信方向、受信方向毎に準備する送信元アドレス、受信元アドレス対応のＳＡ９００を配置する。

第二のノード１０６のソフトウェア構成としては、前記第一のノード１０５のソフトウェア構成から、ユーザインタフェースの為に利用するユーザインタフェース制御部１５１とユーザアクセス制御部２１００を取り除いた構成とする。加えて、グループアクセスデータベース１２０上にアクセスユーザ管理テーブル２００１を配置しない。

図２２に本発明を適用するサブグループ１０８構成を示す。図では、２つのサブグループ

１０８を示している。サブグループ１０８はユーザ対応に利用できるノードをグループ化したものであり、第一のノード１０５からユーザが他のノード１０５、１０６を利用したサービスを実現する場合、ユーザＡはサブグループａ１０８Ａを構成するノード１０５Ａ、１０５Ｂ、１０６Ｃのみ利用でき、ユーザＢがサブグループｂ１０８Ｂを構成するノード１０５Ａ、１０６Ｄ、１０６Ｅのみ利用できる。ユーザＢがノードＡ１０５ＡよりノードＣ１０６Ｃにアクセスするサービスは利用できない。

【０２２９】

ホームネットワークにおいて、ルートグループ１０７上にサブグループ１０８を設定することにより、例えばお父さんのサブグループをＰＣ、テレビ、エアコン、ビデオから構成すると、ＰＣ、テレビからエアコンの温度設定とビデオの予約設定ができる。これに対し、息子のサブグループとして、テレビとビデオを構成することにより、息子はテレビからビデオ予約設定はできるが、エアコンの温度設定はできないといった制御が可能になる。

【０２３０】

以下、このサブグループ１０８の構築方法、及び動作手順を図２３から図３１を用いて説明する。

図２３は、一つのノード１０５、１０６におけるネットワーク接続時の３フェーズを示すものである。第一フェーズは、ノード１０５、１０６をネットワークに繋いだだけの状態であるグループ無しフェーズ２３０１である。グループ無しフェーズ２３０１において、前記実施形態に基づき、ルートグループ１０７生成、ノード１０５，１０６のルートグループ１０７への加入により、第二フェーズであるルートグループフェーズ２３０２となる。この第二フェーズでは、ルートグループ１０７内のノード１０５、１０６間通信において、ルートグループ１０７内で共通のグループ鍵６０２を用いた３ＤＥＳによる暗号通信を行うとする。ルートグループ１０７において、ユーザのアクセス権、及び利用できるノード選択により第三フェーズであるサブグループフェーズ２３０３となる。第三フェーズでは、サブグループ１０８内のノード１０５、１０６間通信において、サブグループ１０８内で共通のグループ鍵６０２を用いた３ＤＥＳの暗号通信を行う。

図２４はグループ管理処理部３０２におけるユーザアクセス制御を行うユーザアクセス制御処理２１００の処理手順を示す図である。ユーザからの要求を受け付ける為、ユーザアクセス制御処理２１００を第一のノード１０５において起動する。本処理は、ユーザが起動させても良いし、ルートグループ１０７に参加した時点で本処理を起動しノード１０５の常駐プログラムとして動作させてもよい。ユーザアクセス制御処理２１００は、ルートグループフェーズ２３０２あるいはサブグループフェーズ２３０３時のみ起動できる（ステップ２１０１）。

ディスプレイに「ユーザアクセス権設定」、「ユーザアクセス権開放」、「サービス利用」を表示し（ステップ２１０２）、ユーザに利用するものを選択してもらい、選択により、ユーザアクセス権設定処理（２１１０）、ユーザアクセス権解放処理（２１３０）、サブグループアクセス権確認処理（２１５０）を実行する。

図２５は、ユーザアクセス権設定処理２１１０の処理手順を示す。

第１ステップとして、グループアクセスデータベース３０８にて管理しているルートグループ１０７に対するグループ管理テーブル６００に登録されているホスト名をディスプレイに表示する（ステップ２１１１）。ルートグループ１０７に対するグループ管理テーブルは、種別６０７のエリアにルートが設定されているとする。

第２ステップとして、ユーザが入力したサブグループ１０８として登録したい複数のホスト名を受け付け、グループアクセスデータベース３０８上に新しいグループ管理テーブル６００をアロケートし、種別６０７をサブとし、ホスト名を登録する（ステップ２１１２）。

第３ステップとして、他のグループ管理テーブル６００のグループ識別子６０１と一致しないグループ識別子６０１を選択し、新しいグループ管理テーブル６００にグループ識別子５０１を設定する（ステップ２１１３）。

第４ステップとして、サブグループ１０８で共通の暗号用のグループ鍵６０２を生成し、

新しいグループ管理テーブル６００に設定し、鍵有効期間と３ＤＥＳを暗号アルゴリズムとして設定する（ステップ２１１４）。
第５ステップとして、サブグループ１０８を構成する全てのネットワーク機器１０５Ｂ、１０６Ｃに対して、サブグループ作成要求フレーム２６０１を作成し送信する（ステップ２１１５）。
【０２３１】
送信フレーム構成を図２６に示すように、サブグループ作成要求を示すコマンド識別子、サブグループのグループ識別子６０１、グループを構成する全ノードのホスト名一覧、サブグループのグループ鍵６０２、その有効期限から構成する。本フレーム２６０１は、ＴＣＰ／ＵＤＰ送信処理部３０３を介してＵＤＰデータグラムとして送信され、ＩＰ送信部３０４においてルートグループ１０７のグループ鍵により暗号化され送信される。各ノードより返送される確認フレーム２６０２により、各ネットワーク機器への送信を確認する。図２６に示すように、確認フレーム２６０２は受信確認を示すコマンド識別子とグループ識別子６０１から構成する。一定時間、確認フレーム２６０２を受信できない場合、サブグループ作成要求フレーム２６０２を再送してもよい。サブグループ作成要求フレーム２６０１を送信する際、ノード１０５、１０６のホスト名から１Ｐアドレスを得るホスト名を含んだリゾルバ要求をＩＰ送信部３１０へ伝える。ＩＰ送信部に３１０備えたホスト名、ＩＰアドレス、及びテーブル登録時間を管理するタイマから構成するリゾルバテーブルを検索し、ホスト名と一致するＩＰアドレスを検索し、要求に対するリターン値とする。テーブル内に該当するホスト名が無い場合、ＩＣＭＰ Ｅｃｈｏ Ｒｑｕｅｓｔ／Ｒｅｐｌｙよりホスト名からアドレスの解決を行い、リゾルバテーブルにホスト名とＩＰアドレスの組を登録すると共に、要求に対するリターン値とする。
【０２３２】
第６のステップとして、サブグループ１０８を構成する全ネットワーク機器に対する送信用のＳＡ９００と受信用ＳＡ９００Ａを作成する（ステップ２１１６）。
図２７にＳＡ９００Ａの構成を示す。
【０２３３】
送信用ＳＡ９００Ａとしては、ＳＰＩとしてグループ識別子６０１を設定し、送信元ＩＰアドレスとして自ネットワーク機器のアドレスを設定し、送信先１ＰアドレスとしてサブグループＩＤを構成する他ネットワーク機器のＩＰアドレスを設定する。本実施形態では、プロトコルとしてＥＳＰを、モードはトランスポート、暗号アルゴリズムは３ＤＥＳ、暗号鍵としてサブグループのグループ鍵６０１を設定する。受信用ＳＡ９００Ａとしては、送信元ＩＰアドレスとして他ネットワーク機器のＩＰアドレスを、送信先１Ｐアドレスとして自ネットワーク機器のアドレスを設定する以外は送信用ＳＡ９００と同じ構成である。
【０２３４】
第７のステップとして、ユーザによるアクセスユーザＩＤとパスワードをデータ入力インタフェース部２０９とデータ出力インタフェース部２０８を介して受け付ける（ステップ２１１７）。
【０２３５】
第８のステップとして認証鍵２００２を生成する（ステップ２１１８）。
【０２３６】
第９のステップとして、ユーザが挿入した空のフォーマット済みのメモリカード２０７上にユーザＩＤ、パスワード、認証鍵２００２、自ネットワーク機器のグローバル１Ｐアドレス、サブグループのグループ識別子６０１を書き込む（ステップ２１１９）。
【０２３７】
第１０のステップとして、グループアクセスデータベース３０８のアクセスユーザ管理テーブル２００１に認証鍵２００２、ユーザＩＤ、サブグループのグループ識別子を設定する（ステップ２１２０）。
【０２３８】
ユーザアクセス権設定処理２１１０の最終である第１１のステップとして、サブグループ

１０８を構成する全てのノードに対して、サブグループアクセス権設定フレーム２６０３を作成し送信する（ステップ２１２１）。

【０２３９】

送信フレーム構成を図２６に示すように、サブグループアクセス権設定を示すコマンド識別子、サブグループのグループ識別子６０１、ユーザＩＤ、認証鍵２００２、パスワードから構成し、上述したサブグループ設定要求フレーム７０１と同様の手順で送信及び送信確認を行う。

【０２４０】

次にサブグループ設定要求フレーム２６０１、及びサブグループアクセス権設定フレーム２６０３を受信したサブグループを１０８を構成するノード１０５、１０６におけるグループ管理処理部３０２でのサブグループ管理処理２２００で行われる処理手順を図２８に示す。

【０２４１】

サブグループ設定処理２２００は、ルートグループフェーズ２３０１あるいはサブグループフェーズ２３０３時のみ起動できる（ステップ２２０１）。

サブグループ設定要求フレーム２６０１を受け付けた場合、グループ管理テーブル６００をアロケートし、フレームが持つ情報を設定する。次に送信用ＳＡ９００と受信用ＳＡ９００をユーザアクセス権設定処理２１１０で示したように作成する（ステップ２２０２）。

【０２４２】

サブグループアクセス権設定フレーム２６０３を受け付けた場合、自ノードが第一のノード１０５である場合は、グループアクセスデータベース３０８のアクセスユーザ管理テーブル２００１をアロケートし、フレームが持つ情報であるグループ識別子、ユーザＩＤ、認証鍵、パスワードを設定する（ステップ２２０３）。

サブグループ設定要求フレーム２６０１、サブグループアクセス権設定フレーム２６０３の受信確認として、図２６に示す受信確認フレーム２６０２を返送する（ステップ２２０３）。

【０２４３】

以上によりサブグループの構築が完了する。

【０２４４】

次にサブグループアクセス権開放処理２１５０の手順を示す。

管理者あるいはユーザがサブグループアクセス権開放を選択した場合、図２６に示す、サブグループ解放要求を示すコマンド識別子とサブグループのグループ識別子６０１から構成するサブグループ解放要求フレーム２６０４をサブグループ構成する全てのネットワーク機器に対して送信する。その後、管理者により指定されたサブグループのグループ識別子６０１を持つグループ管理テーブル６００、アクセス及びセキュリティアソシエーションを解放し、対応するアクセスユーザ管理テーブル２００１の対応欄を削除する。

【０２４５】

本フレームを受信したグループ管理処理部３０２でのサブグループ管理処理２２００において、図２８に示すように、受信したフレームにより指示されたサブグループ識別子６０１を持つグループ管理テーブル６００とＳＡ９００を削除し（ステップ２２０５）、自ノードが第一のノード１０５である場合、アクセスユーザ管理テーブルの対応欄を削除する（ステップ２２０６）。

【０２４６】

以上の手順により、作成したサブグループを解放することができる。

以下、サブグループ１０８における通信手順を図２９から図３１を用いて説明する。

【０２４７】

サブグループ１０８をユーザが利用する場合の手順を示す。

ユーザアクセス制御処理２１００より、ディスプレイに表示された「ユーザアクセス権設定」、「ユーザアクセス権開放」、「サービス利用」から、ユーザは、「サービス利用」

を選択する（ステップ２１０２）。
【０２４８】
複数のサービスを提供出来る場合、この選択時に一つのサービスを選択させても良い。上記選択により、サブグループアクセス権確認処理２１５０を行う。
図２９において、サブグループアクセス権確認処理２１５０の処理手順を示す。第１のステップとして、ユーザにユーザＩＤ、パスワード、認証鍵を記憶したメモリカード２０７の挿入を指示する（ステップ２１５１）。
【０２４９】
ユーザがメモリカード２０７の挿入を受け、第２のステップとして、メモリカード２０７上のユーザＩＤと対応するグループアクセスデータベース３０８上のアクセスユーザ管理テーブル２００１を検索し、メモリカード上のメモリカードが記憶しているパスワードとアクセスユーザ管理テーブル２００１のパスワードが一致することを確認する（ステップ２１５２）。
【０２５０】
ユーザＩＤが一致するアクセスユーザ管理テーブル１２１が無い場合、あるいはパスワードが不一致の場合、認証エラーをディスプレイに表示し、処理を終了する（ステップ２１５３）。
【０２５１】
第３のステップとして、ユーザが指定したサービスに対応するアプリケーションを起動し、アプリケーションがデータ送受信に利用するソケットに割り付けた送信ポート番号を入手する（ステップ２１５４）。
メモリカード上のグループ識別子６０１と一致するグループ管理テーブル６００のポート番号エリア６０８にソケットに割付けた送信ポート番号を設定する（ステップ２１５５）。
【０２５２】
第４のステップとして、ノードがユーザアクセス状態プロセス２３００を起動し、サブグループアクセス権確認処理を終了する（ステップ２１５６）。
本実施形態では、アプリケーションプログラム３０１では、初期処理として、データ転送を行うためにソケットをオープンすると同時に送信元ポート番号をソケット処理部から割り付けられる為、サブグループアクセス権確認処理２１５０に通知できるとする。
【０２５３】
図３０にユーザアクセス状態プロセス２３００の処理手順を示す。
ユーザアクセス状態プロセス２３００では、ユーザがメモリカード２０７を外した事を検出し、サブグループ１０８のアクセス権を終了するため、グループアクセス権確認処理２１５０においてグループ管理テーブル６００に設定した送信元ポート番号を削除する（ステップ２３０１）。
【０２５４】
これにより、ユーザによるサブグループ３０１利用を中止する事が可能である。
次に、ユーザが指定したアプリケーションによるサブグループ内の１Ｐパケット送受信手順を示す。
【０２５５】
図３１は、ＩＰｓｅｃ送信処理部３０６の処理手順を示すものである。
第１のステップとして、送信パケットの送信元ＩＰアドレスと送信先アドレスが一致するＳＡをＳＡデータベースより検索する（ステップ４１０１）。
第２のステップとして、ユーザアクセス状態プロセス２３００が起動中でなければ、ＳＡ９００の種別がルートであるものを検索する（ステップ４１０２）。送信元ＩＰアドレス、受信元ＩＰアドレスが一致したＳＡ９００のグループ識別子６０１を持つグループ管理テーブル６００の種別６０７により、ルートグループ１０７であるか否かを判断する。
【０２５６】
そのＳＡ９００が管理しているグループ鍵６０２を用いて、１Ｐパケットの暗号化を行い

ＩＰｓｅｃ送信処理を行う（ステップ４１０３）。
ユーザアクセス状態プロセス１１００が起動中であれば、第３のステップとして、ＳＡ９００の種別がサブであるものを検索し（ステップ４１０４）、検索したＳＡ９００のＳＰＩに対応するグループ管理テーブル１２２のポート番号と送信パケットＴＣＰあるいはＵＤＰヘッダの送信元ポート番号が一致するかどうかを調べ（ステップ４１０５）、一致した場合、そのＳＡ９００を用いてＩＰｓｅｃ送信処理４１０３を行う。
【０２５７】
一致するＳＡが無い場合、処理を終了する。この場合、ＩＰｓｅｃ処理を行わずにＩＰパケットが送信される為、次に示す手順により受信側のアクセス制御により、ルートグループあるいはサブグループの通信以外として破棄される。
次に、図３１に示す手順で送信したＩＰパケットを受信した場合のＩＰｓｅｃ受信処理手順を示すものである。ＩＰ受信部３１４のＩＰｖ６受信前処理部３１１において、ＡＨヘッダあるいはＥＳＰヘッダが受信パケットにある場合ＩＰｓｅｃ受信処理部３１２は起動される。
【０２５８】
ＩＰｓｅｃ受信処理部３１２では、ＡＨヘッダあるいはＥＳＰヘッダに含まれるＳＰＩと一致するＳＡをＳＡデータベースより検索する。検索したＳＡデータベースに含まれる暗号鍵により復号処理を行う。
【０２５９】
ＡＨヘッダあるいはＥＳＰヘッダが無い場合、受信アクセス制御部３１６により、ＩＰｓｅｃ通信が行われていなくても、アクセス制御対象アプリケーション管理テーブル７００に登録されているポート番号と受信パケットの送信先ポート番号を比較し、一致している場合は、上位処理部にあたるＴＣＰ／ＵＤＰ受信処理部３１５へパケットを引き渡す。それ以外のＩＰパケットは、ＩＣＭＰパケット等の制御パケットでなければ、ルートグループあるいはサブグループ対象外のパケットとして、受信ＩＰパケットを破棄する。
【０２６０】
図３１に示すＩＰｓｅｃ送信処理では、送信パケットに対応するＳＡ９００検索時に、グループ管理テーブル６００の種別がサブであり、ポート番号が送信パケットの送信元ポート番号が一致することによりＳＡ９００の特定を行っているが、グループアクセスデータベース３０８内にサブグループ識別子を記憶するアクティブエリアを設け、図２９における対応するグループ管理テーブル６００にアプリケーション起動時に得る送信元ポート番号を記憶する（ステップ２１５４、２１５６）代わりに、前記アクティブエリアにメモリカード２０７に記憶されているグループ識別子６０１を設定し、１Ｐｓｅｃ送信処理１３２では、前記アクティブエリアのグループ識別子６０１とＳＡ９００のＳＰＩが一致することにより、ＳＡ９００を特定することも可能である。
【０２６１】
この場合、複数のアプリケーションプログラム３０１を同時動作させている場合でも前記アクティブエリアにおいて、グループ識別子６０１だけを管理すれば良い。
【０２６２】
これに対し、グループ管理テーブル６００でポート番号を管理する場合、アプリケーションプログラム３０１に対応した複数のポート番号が必要である。
【０２６３】
このように、共通鍵を備えた複数のノード１０５、１０６でＩＰｓｅｃ通信を行うノードから構成するルートグループ１０７において、ユーザインタフェースを備えた第一のノード１０５から制御する複数のノード１０５、１０６から構成するサブグループ１０８を構成し、そのサブグループ１０８内で共通の第二の暗号鍵によりＩＰｓｅｃ通信を実現できるように、第一のノード１０５において、サブグループ設定時にサブグループの共通暗号鍵及び記憶媒体２０７に記憶するユーザアクセス情報を他の第一及び第二のノード１０５、１０６に対し、ルートグループ１０７の暗号通信を用いて転送し、サブグループ１０８を構築する。

【０２６４】
これにより、サブグループ１０７を構成するノード１０５、１０６において、サブグループ１０８のグループ鍵を設定したＳＡ９００を設定し、ユーザが第一のノード１０５より利用する場合、記憶媒体２０７をノード１０５に入れ、ユーザの認証、利用するサブグループ１０８を識別、利用するアプリケーション３０１のポート番号６０８をノード１０５において記憶する手段を備え、ノードから送信する際には、ＩＰｓｅｃ送信処理において、ＳＡ９００検索時に、前記ポート番号と送信パケットのＵＤＰあるいはＴＣＰヘッダを構成する送信元ポート番号が一致している場合、そのＳＡ９００を用いて転送を行うことにより、サブグループ１０８内だけの通信及びグループへのユーザアクセス制御を実現できる。

【０２６５】
次に図３２から図３６を用いて、外部ネットワークからのサブグループへのアクセス権を備えたユーザがサブグループへのアクセスを実現する手順を示す。
図３２は、本実施形態のシステム構成の一例を示す図である。

【０２６６】
宅内ネットワーク及び外部ネットワーク、外部ネットワークに接続しているホスト４２０１、宅内ネットワークを構成するノード１０５Ａ、１０６Ｂ、１０６Ｃ、１０６Ｄから構成し、これらのノード１０５、１０６は、ルートグループ１０７を構成している。本構成では、ノードＡ１０５Ａがユーザインタフェースを備えた第一のノードとし、上述した実施形態の手順に従い、ノードＡ１０５Ａ，ノードＢ１０６Ｂ，ノードＣ１０６Ｃから構成するサブグループ１０８を構築しているとする。

【０２６７】
サブグループ１０８へのアクセス権を持ったユーザが、ユーザＩＤ、パスワード、認証鍵等を格納しているメモリカード２０７を持って、ホスト３２０１からサブグループ１０８をアクセスする手順を示す。

【０２６８】
ホスト４２０１上には、サブグループへのアクセス制御を実現するためのサブグループアクセスクライアント処理４３０１を行うソフトウェアを予め実装してあるとし、ユーザにより起動されるとする。

【０２６９】
サブグループクライアント処理４３０１の処理手順を図３３に示す。
第１のステップとして、前記メモリカードの２０７挿入指示、及びユーザＩＤとパスワードの入力をユーザに対してディスプレイ表示により指示する（ステップ４３０２）。

【０２７０】
メモリカード２０７の挿入、及びユーザからのユーザＩＤとパスワードの入力を受けて、第２のステップとして、メモリカード２０７上のユーザＩＤ、パスワードと入力値が一致していることを確認する（ステップ４３０３）。
一致していない場合、ユーザ認証エラーを表示して処理を終了する（ステップ４３０４）。

【０２７１】
一致した場合、第３のステップとして、ユーザＩＤとパスワードを認証鍵２００２で演算を行った認証情報を図３４に示す認証情報フレーム４４０１として、ＵＤＰあるいはＴＣＰパケットとして、メモリカード２０７に記憶しているＩＰアドレスを送信先アドレスとして送信する（ステップ４３０５、ステップ４３０６）。

【０２７２】
前記演算に関しては、共通鍵暗号方式である暗号アルゴリズムの３ＤＥＳを用いるとする。

【０２７３】
第４のステップとして、認証情報フレーム４４０１に対して、ノードＡ１０５Ａにより返送される図３４に示す認証アクセプトフレーム４４０２の受信を待つ（ステップ４３０７

）。
【０２７４】
第５のステップとして、フレームを受信した場合、ステートがＯＫであれば、フレームが持つ認証グループ鍵情報をメモリカード上の認証鍵１２６で復号化しサブグループのグループ鍵１２４を入手する（ステップ４３０８）。
ステートがＮＧであれば、ユーザ認証エラーをディスプレイに表示し処理を終了する（ステップ４３０４）。
【０２７５】
第６のステップとして、メモリカード２０７上のＩＰアドレスを送信元／送信先としたサブグループ３０１のグループ鍵１２４を設定した送信用ＳＡ９００と受信用ＳＡ９００を作成する（ステップ４３１０）。
【０２７６】
以上により、宅内ネットワークのサブグループ１０８のグループ鍵６０１を外部ネットワークに接続したホスト４２０１と共有できるため、サブグループ１０８を構成するノードＡ１０５Ａとの通信においてサブグループのグループ鍵６０１を用いた暗号通信が可能になる。
【０２７７】
本クライアント処理では、メモリカード２０７が離脱された時点で、サブグループ１０８へのアクセス権が無くなったとして、第７のステップとして、ノードＡ１０５Ａに対し図３４に示すアクセス権解放フレーム３４０３をノードＡ１０５Ａに対し送付する（ステップ４３１１）。
【０２７８】
ホスト４２０１から送付するパケットに関しては、図３４に示す受信確認フレーム４４０４を用いて、フレームの送達確認を行ってもよい。
第８のステップとして、第６のステップで作成したＳＡ９００を解放する（ステップ４３１２）。
【０２７９】
外部ネットワークからのアクセスを受け付ける第一のノード１０５Ａにおけるグループ管理処理部３０２の処理構成を図３５に示す。
【０２８０】
グループ管理処理部３０２は、サブグループ管理処理２２００、ユーザアクセス制御処理２１００に加え、外部ネットワークからのアクセスを受け付ける為のリモートアクセス制御処理２５００、外部ネットワークからのサブグループを構成するネットワーク機器を利用するためのアプリケーションプログラムを起動する為のアプリケーションプロキシ２４００から構成する。
【０２８１】
図３６にリモートアクセス制御処理２５００における処理手順を示す。
リモートアクセス制御処理２５００は、外部ネットワークのホスト４２０１からのフレームを受信した場合に起動される。
【０２８２】
外部ネットワークのホスト４２０１からのフレームであることは、送信元ＩＰアドレスのサブネットプリフィクスが宅内ネットワークに割り付けられたサブネットプリフィクスと異なることから判断できる。
【０２８３】
グループ通信では、ＩＰｓｅｃでの暗号化通信していない場合、グループ外のネットワーク機器からの通信で有るためＩＰパケットは受信アクセス制御部３１６で破棄される事を避けるため、予めアクセス制御対象アプリケーション管理テーブル７００にリモートアクセス制御処理２３００のポート番号を登録しておく。これは、グループ管理処理部３０２を起動した際の初期化処理で割り付けたポート番号、あるいは固定したポート番号を登録する。

【０２８４】
受信フレームが、図３４に示す認証情報フレーム４４０１の場合、アクセスユーザ管理テーブルより認証情報フレーム４４０１のサブグループのグループ識別子６０１と一致する認証鍵２００２でフレーム４４０１認証情報を復号し、ユーザＩＤとパスワードを取り出す（ステップ２５０１）。
【０２８５】
このユーザＩＤとパスワードがサブグループ識別子６０１と一致するアクセスユーザ管理テーブル２００１が持つ値と一致していることを確認する（ステップ２５０２）。
【０２８６】
一致しなければ、パケットを破棄し、ステートをＮＧとした図３４に示す認証アクセプトフレーム４４０２を返送し、処理を終了する（ステップ２５０３）。
一致している場合対応するサブグループ１０８のグループ管理テーブル６００のグループ鍵６０２を認証鍵２００２で暗号化したグループ鍵情報と、ステートをＯＫとした図３４に示す認証アクセプトフレーム４４０２として、ホスト４２０１へ返送する（ステップ２５０４）。
【０２８７】
ホスト４２０１のＩＰアドレスを送信元／送信先としたサブグループ１０８のグループ鍵６０２を設定したＳＡ９００を作成する（ステップ２５０５）。
ノードＡ１０５Ａが提供するアプリケーションをホスト４２０１で利用できるようにするため、アプリケーションプロキシ処理２４００を起動する（ステップ２５０６）。
【０２８８】
ホスト４２０１からアクセス権解放コマンド４４０３を受信した場合、図３４に示す確認フレーム４４０４をホスト４２０１へ返送し（ステップ２５０７）、ホスト４２０１とノード１０５Ａ間のＳＡ９００を解放し（ステップ２５０８）、対応するグループ管理テーブル６００のポート番号を削除し（ステップ２５０９）、アプリケーションプロキシ処理２４００を終了する（ステップ２５１０）。
【０２８９】
さらに、ホスト４２０１からアクセスされたサブグループ１０８のグループ鍵６０２を更新する（ステップ２５１１）。
【０２９０】
これにより、サブグループアクセスの鍵情報がホスト４２０１に残っていたとしても、サブグループにアクセスすることは出来ない。
【０２９１】
図３７にアプリケーションプロキシ処理２４００の処理手順を示す。
【０２９２】
アプリケーションプロキシ処理２４００は、例えばＷｅｂサーバとして動作しており、外部ネットワークに接続するホスト４３０１とノードＡ１０５Ａ間はＨＴＴＰベースで通信を行うとする。まず、アプリケーションプロキシ処理１１４として、サブグループ３０１を構成する。
【０２９３】
次に、第１のステップとして、ユーザに対し、利用できるサービスアプリケーション情報を通知する（ステップ２４０１）。
【０２９４】
第２のステップとして、ユーザからの利用するサービスアプリケーションの指定を受け、対応するアプリケーションプログラム３０１をノードＡ１０５Ａにおいて起動し、送信元ポート番号を上述した実施形態に即して、入手する（ステップ２４０２）。
【０２９５】
第１のステップ、第２のステップにおけるホスト４３０１とノードＡ１０５Ａ間はＨＴＴＰベースである。
【０２９６】

第３のステップとしての入手した送信元ポート番号を対応するグループ識別子６０１を持つグループ管理テーブル６００に登録する（ステップ２４０３）。
ノードＡ１０５Ａのアプリケーションプログラム３０１は、ホスト４３０１よりアプリケーションプロキシ処理２４００を介して操作する（ステップ２４０４）。具体的には、アプリケーションプロキシでアプリケーションに対する交信をノードに代替して行う。ノードＡ１０５Ａのアプリケーションプログラム３０１からサブグループ１０８を構成する他のノード１０６Ｂ、１０６Ｃへの要求は、上述した実施形態である図３１のＩＰｓｅｃ送信処理手順に従い、サブグループ通信のアクセス制御を行う。

【０２９７】

また、図２５のユーザアクセス権確定処理２１１０において、メモリカード２０７の記憶情報として、サブグループ１０８を構成するノード１０５、１０６のアドレスとホスト名をメモリカード２０７に記憶させ、第二のノード１０６において、グループアクセスデータベース３０５にアクセスユーザ管理テーブル２００１をサブグループアクアクセス権確定フレーム２６０３受信時に作成させ、かつ図３５に示すグループ管理処理部３０２において第一のノード１０５と同様に、リモートアクセス制御処理２５００及びアプリケーションプロキシ処理２４００を行うことにより、ホスト４３０１において、メモリカード２０７に記憶されているホスト名をユーザが選択する事によりサブグループ１０８を構成する全てのノード１０５Ａ、１０６Ｂ、１０６Ｃに直接アクセスすることが可能になる。

【０２９８】

このような処理手順により、外部ネットワークに位置するホストとサブグループを構築したノード間でユーザアクセス認証を実現すると共に、サブグループの共通鍵をホストに配布することにより、特別な認証サーバを配置することなく、宅内ネットワークのグループ通信に参加することができる。

【０２９９】

本実施形態によれば、前記グループ通信を行うネットワーク機器から、ユーザが利用できるネットワーク機器を選択し、その選択したネットワーク機器で利用する共通の第二の暗号鍵を前記の暗号鍵（第一の暗号鍵）で暗号化して配布することにより、ユーザ独自の第二のグループ通信を実現することができる。
また、第二の暗号鍵と対応したユーザの識別子とパスワードの情報をネットワーク機器と記憶媒体で管理すると共に、第二の暗号鍵の識別子を記憶媒体で管理し、ネットワーク機器では第二の暗号鍵と対で前記識別子を管理し、第一の暗号鍵で前記情報を暗号化して他の第二のグループ通信を行うネットワーク機器へ配布することにより、ユーザがネットワーク機器を利用する際、どのネットワーク機器においても、記憶媒体の情報とネットワーク機器の情報が一致することを確認し、ユーザが通信する際、記憶媒体の識別子と対になる第二の共通の暗号鍵で暗号通信によるグループ通信をすることにより、グループ通信へのユーザの利用可否を制御できる。

【０３００】

また、ユーザが利用するアプリケーションの送信元ポート番号を記憶し、パケット送信時にパケットの送信元ポート番号と記憶した送信元ポート番号を比較し、一致した場合のみ第二の共通の暗号鍵で暗号通信を行うことにより、受信側では暗号化されたパケットでなければ破棄することによる、グループ通信への利用可否を制御できる。

【０３０１】

さらに、本実施形態では、記憶媒体でネットワーク機器のアドレスと認証鍵を管理し、ネットワーク機器において認証鍵を管理し、第一の暗号鍵で暗号化して他の第二のグループ通信を行うネットワーク機器へ管理を依頼することにより、グループ通信対象でないネットワーク機器からユーザが第二のグループ通信対象のネットワーク機器と通信を開始する際、記憶媒体の認証鍵で、記憶媒体のパスワードとユーザＩＤを暗号化し、その暗号化情報を記憶媒体のアドレス宛てに送信し、第二のグループ通信対象のネットワーク機器では認証鍵でユーザＩＤとパスワードを復号化し、ユーザＩＤとパスワードを確認した上で、第二の共通の暗号鍵を認証鍵で暗号化して、返送することにより、グループ通信対象でな

いネットワーク機器との間で第二の暗号鍵での暗号通信を実現できる。

【０３０２】

【発明の効果】

本実施形態においては、特別に認証サーバまたは鍵管理手段を備えた装置を保有しなくても、グループを構成する機器間で、互いにグループ構成機器であることを認証し、安全な通信を実現するグループを容易に生成し、管理することができる。

【０３０３】

また、機器がグループ内の機器にのみ提供するアプリケーションとグループ外の機器に提供するアプリケーションとを有する場合、そのアクセス制御を簡単な構成にて行なうことができる。

【図面の簡単な説明】

【図１】本発明を適用した実施形態のシステム構成を示す図である

【図２】本実施形態におけるノードのハードウェア構成を示す図である。

【図３】本実施形態におけるノードにおけるソフトウェア構成を示す図である。

【図４】グループ通信に用いるＡＨヘッダ付きのＩＰパケットの構成を示す図である。

【図５】グループ通信に用いるＥＳＰヘッダ付きのＩＰパケットの構成を示す図である。

【図６】本実施形態のおけるグループ管理処理部の機能構成を示す図である。

【図７】本実施形態におけるグループ制御ＩＰパケットのデータ部の構成の一例を示す図である。

【図８】グループ管理テーブルの構成の一例を示す図である。

【図９】アクセス制御対象アプリケーション管理テーブルの構成の一例を示す図である。

【図１０】グループメンバ管理テーブルの構成の一例を示す図である。

【図１１】セキュリティアソシエーションとして設定する情報構成の一例を示す図である。

【図１２】グループ管理処理の処理手順を示す図である。

【図１３】グループ生成処理の処理手順を示す図である。

【図１４】グループ参加処理の処理手順を示す図である。

【図１５】グループ内への新メンバ通知処理の処理手順を示す図である。

【図１６】グループ離脱処理の処理手順を示す図である。

【図１７】グループ制御ＩＰパケット受信処理の処理手順を示す図である。

【図１８】ＩＰパケット受信時のＩＰ受信部の処理手順を示す図である。

【図１９】ＩＰパケット受信時の受信アクセス制御部の処理手順を示す図である。

【図２０】ネットワーク機器のソフトウェア構成とネットワーク機器から構成するネットワークシステムを示す図である。

【図２１】ハードウェア構成及び記憶媒体の記憶情報を示す図である。

【図２２】第一のグループ通信と第二のグループ通信の範囲を示す図である。

【図２３】グループ通信を行うネットワーク機器の接続フェーズを示す図である。

【図２４】グループ管理処理部におけるユーザアクセス制御を行う処理手順を示す図である。

【図２５】ユーザアクセス権設定処理の処理手順を示すを示す図である。

【図２６】ユーザアクセス権設定処理の処理にて他のグループ通信を行うネットワーク機器間でやり取りされるフレーム構成を示す図である。

【図２７】ＳＡの一構成例を示す図である。

【図２８】グループ管理処理部でのサブグループ管理処理手順を示す図である。

【図２９】サブグループアクセス権確認処理の処理手順を示す図である。

【図３０】ユーザアクセス状態プロセスの処理手順を示す図である。

【図３１】ＩＰｓｅｃ送信処理部の処理手順を示す図である。

【図３２】本発明を適用するシステム構成の一例を示す図である。

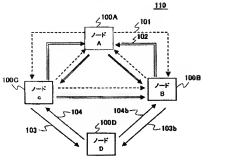
【図３３】サブグループアクセスクライアント処理の処理手順を示す図である。

【図３４】ホストとノード間でやり取りされるフレーム構成を示す図である。

【図３５】第一のノードにおけるグループ管理処理部の処理構成を示す図である。
【図３６】リモートアクセス制御処理における処理手順を示す図である。
【図３７】アプリケーションプロキシ処理における処理手順を示す図である。
【符号の説明】
１００、１０５、１０６…ノード、１０７…ルートグループ、１０８…サブグループ、２０７…メモリカード、３０１…アプリケーション、３０２…グループ管理処理部、３０８…アクセスポリシデータベース、３０９…ＳＡデータベース、３１４…ＩＰ受信部、３０４…ＩＰ送信部、３１２…ＩＰｓｅｃ受信処理部、３１６…受信アクセス制御部、６００…グループ管理テーブル、７００…アクセス制御対象アプリケーション管理テーブル、８００…グループメンバ管理テーブル、９００…セキュリティアソシエーション、２００１…アクセスユーザ管理テーブル、２００２…認証鍵、２１００…ユーザアクセス制御処理、２１５０…サブグループアクセス権確認処理、２２００…サブグループ管理処理、２４００…アプリケーションプロキシ処理、２５００…リモートアクセス制御処理、３１００…制御部、３２００…　グループ生成処理部、３３００…グループ参加処理部、３４００…グループ離脱処理部、３５００…グループ情報更新処理部、３６００…グループ制御ＩＰパケット受信処理部、４２０１…ホスト、４３０１…サブグループアクセスクライアント処理。

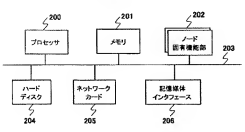
【図１】

図1



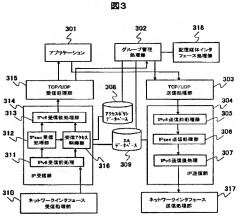
【図２】

図2



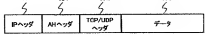
【図３】

図3



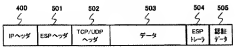
【図４】

図4



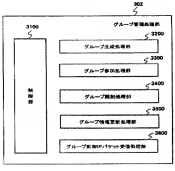
【図５】

図5



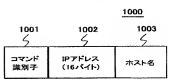
【図６】

図6



【図７】

図7



【図８】

図8

グループ管理テーブル

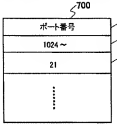
800

グループ識別子	801
グループ鍵	802
鍵有効期間	803
IPsec 種別（認証／暗号）	804
アルゴリズム	805
ホスト名1	806A
⋮	
ホスト名n	806B

【図９】

図9

アクセス制御対象アプリケーション管理テーブル



【図１０】

図10

グループメンバ管理テーブル 800

801 ホスト名	802 IPアドレス	803 有効期間
ノードA	FE 80 :: 68 12 54 FE 35 01	＊＊＊＊
⋮	⋮	⋮

【図１１】

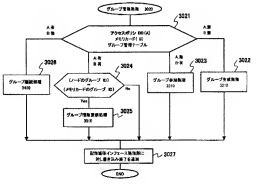
図11

セキュリティアソシエーション 900

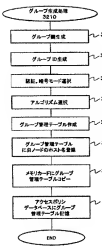
SPI	グループ識別子
宛先先IPアドレス	FE 80 :: 68 12 54 FE 35 01
送信元IPアドレス	FE 80 :: 68 12 54 FE 20 02
プロトコル	AH
モード	トランスポート
暗号アルゴリズム	――
暗号鍵	――
認証アルゴリズム	SHA-1
認証鍵	グループ管理テーブル上のグループ鍵
有効期間	＝7.4sec

【図１２】

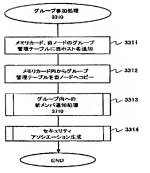
図12



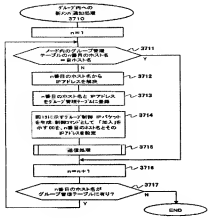
【図１３】



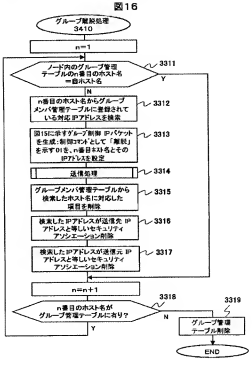
【図１４】



【図１５】



【図１６】

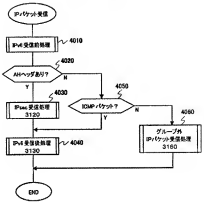


【図１７】

図17

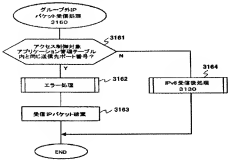
【図１８】

図18



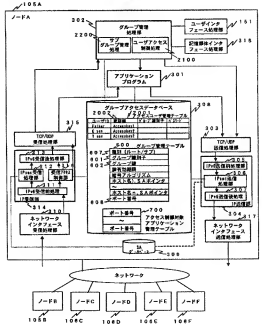
【図１９】

図19

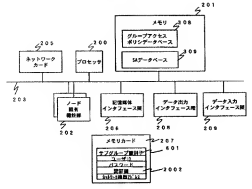


【図２０】

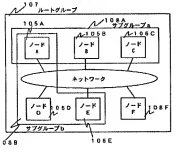
図20



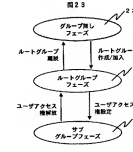
【図２１】



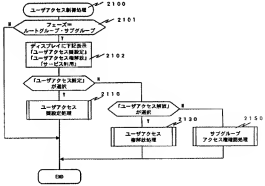
【図２２】



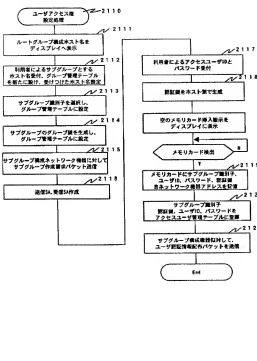
【図２３】



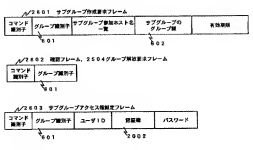
【図２４】



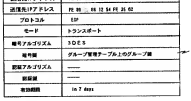
【図２５】



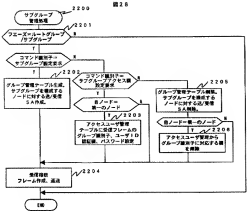
【図２６】



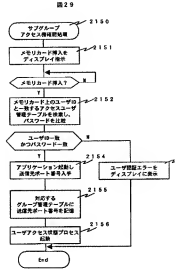
【図２７】



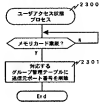
【図２８】



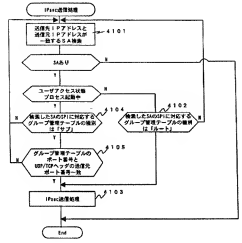
【図２９】



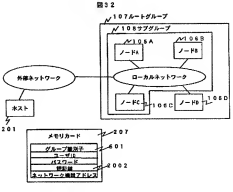
【図３０】



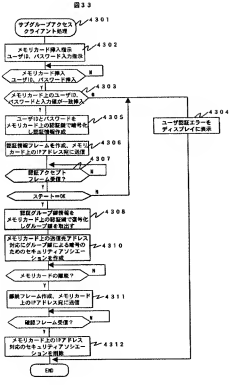
【図３１】



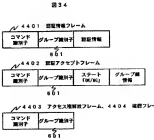
【図３２】



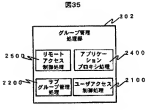
【図３３】



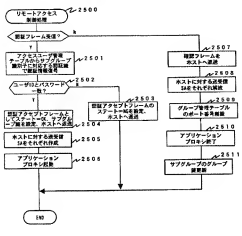
【図３４】



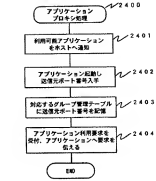
【図３５】



【図３６】



【図３７】



フロントページの続き

(72)発明者 海老名 明弘
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所システム開発研究所内

Ｆターム(参考) 5J104 AA07 AA16 EA02 EA04 EA15 EA18 EA22 JA03 KA02 KA04
MA07 NA02 NA24 NA27 NA33 NA37 PA07